NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

ENHANCING FBI TERRORISM AND HOMELAND SECURITY INFORMATION SHARING WITH STATE, LOCAL AND TRIBAL AGENCIES

by

Peter L. Gomez

September 2010

Thesis Advisor:	Robert Josefek
Second Reader:	Edward J. Valla

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2010	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Enhancing FBI Terrorism and Homeland Security Information Sharing With State, Local and Tribal Agencies		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Peter L. Gomez			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) Federal Bureau of Investigation - Boston Division 1 Center Plaza, Suite 600 Boston, Massachusetts		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number _____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE**	

13. ABSTRACT (maximum 200 words)

This thesis examines FBI terrorism and homeland security information sharing with state, local and tribal homeland security agencies mandated by presidents Bush and Obama, and the U.S. Congress. The thesis compares this "status quo" with three new proposed approaches that use technology and modify the FBI "routine use" exceptions to the Privacy Act to improve overall FBI information sharing. The thesis rates the following approaches: (1) "status quo," (2) new homeland security "routine use" exception, (3) Discoverability of Information and (4) XML Segregation of Information. All four options are analyzed using a two-phase analysis to determine their effectiveness and likelihood of successful implementation. The effectiveness is evaluated by judging the information shared, the privacy protected and the security of each approach. The likelihood of successful implementation is evaluated by judging the impact of FBI cultural resistance, fiscal performance, utilization of technology and training requirements. This thesis proposes the implementation of all three proposed approaches to enhance overall FBI terrorism and homeland security information sharing.

14. SUBJECT TERMS Information Sharing; Federal Bureau of Investigation, Privacy Act of 1974, "routine use" exceptions; Extensible Markup Language (XML); homeland security information; terrorism information, pointer system; Law Enforcement National Data Exchange (N-DEx); FBI Culture	**15. NUMBER OF PAGES** 145
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

ENHANCING FBI TERRORISM AND HOMELAND SECURITY INFORMATION SHARING WITH STATE, LOCAL AND TRIBAL AGENCIES

Peter L. Gomez
Supervisory Special Agent, Federal Bureau of Investigation
B.A., University of Central Florida, 1992
J.D., DePaul University, 1995

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
September 2010

Author: Peter L. Gomez

Approved by: Robert Josefek, PhD
Thesis Advisor

Edward J. Valla, PhD
Second Reader

Harold A. Trinkunas, PhD
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis examines FBI terrorism and homeland security information sharing with state, local and tribal homeland security agencies mandated by Presidents Bush and Obama, and the U.S. Congress. The thesis compares this "status quo" with three new proposed approaches that use technology and modify the FBI "routine use" exceptions to the Privacy Act to improve overall FBI information sharing. The thesis rates the following approaches: (1) "status quo," (2) new homeland security "routine use" exception, (3) Discoverability of Information and (4) XML Segregation of Information. All four options are analyzed using a two-phase analysis to determine their effectiveness and likelihood of successful implementation. The effectiveness is evaluated by judging the information shared, the privacy protected and the security of each approach. The likelihood of successful implementation is evaluated by judging the impact of FBI cultural resistance, fiscal performance, utilization of technology and training requirements. This thesis proposes the implementation of all three proposed approaches to enhance overall FBI terrorism and homeland security information sharing.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

The 9/11 attacks required extensive reviews of the failures that contributed to this successful surprise attack inside the United States by Al Qaeda. Two major commissions concluded that information sharing is crucial for preventing another terrorist attack and protecting the United States. This view is also widely held by not only the president, but also most others in the national command structure of the U.S. government. The FBI responded to these mandates with numerous "ad hoc" approaches to enhance sharing of FBI terrorism and homeland security information. These ad hoc approaches created a "status quo" within the FBI that relies on numerous manual methods of information sharing with federal, state, local and tribal agencies. One of the primary limitations of this information sharing is the limitation on sharing personally identifiable information (PII) imposed on federal agencies by the Privacy Act of 1974. The FBI could expand terrorism and homeland security information sharing with other agencies by creating a new "routine use" exception, which permits the FBI to share PII for certain, published "routine uses."

The FBI information sharing "status quo" is a dramatic improvement over the extremely limited information sharing efforts prior to 9/11. The legal and technological limitations of the current FBI "status quo" information sharing efforts necessitate the consideration of other options to further improve FBI information sharing with state, local and tribal (SLT) agencies. The first option considered is the creation of a new homeland security "routine use" exception, which permits the sharing of PII necessary to resolve a predicated terrorist threat (i.e., allegation or information supporting a terrorist threat). The second option is the Discoverability of Information approach, which indexes PII and other sensitive information in FBI case management systems for retrieval by outside SLT agencies through a technological solution. The Discoverability of Information approach provides a reference number for the information, which enables the SLT agency to request this specific information from the FBI. The final option examined in this thesis is the XML Segregation of Information approach, which uses XML technology to segregate different types of information in the original reporting

documents. This technology enables the FBI to create systems to share or protect the appropriate types of sensitive information with the particular outside agency or user.

The "status quo" and the three proposed approaches were examined and compared using a two-phase analysis. The first phase examines the effectiveness of the particular approach by rating performance or anticipated performance on the following factors: (1) information shared, (2) privacy protected and (3) security. These factors are analyzed by rating relevant criteria performance as low, medium or high. All systems passed the ratings for each of the effectiveness factors, and proceeded to the second phase. The second analysis phase examines the likelihood of successful implementation of these approaches by analyzing FBI cultural resistance, fiscal performance, utilization of technology and training for each approach. The XML Segregation of Information approach outperformed all other options in this two-phase analysis. The new homeland security "routine use" exception outperformed all other approaches on the information shared factor. The Discoverability of Information approach also improved performance of information sharing over the "status quo." Ultimately, all three options resulted in some improvement over the "status quo" approach currently employed by the FBI.

Combinations of these individual approaches are examined to determine if multiple approaches would outperform any individual approach. The analysis of combination approaches results in the final thesis recommendation for the FBI to implement all three approaches to create a systematic, technological approach to dramatically improve information sharing with SLT agencies. The combination of all approaches allows for the maximum sharing of terrorism and homeland security information with the new homeland security "routine use" exception, through the two technological approaches. The Discoverability of Information approach enables the best information sharing performance for the FBI historical information, while the XML Segregation of Information approach enables the FBI to maximize the sharing of newly collected terrorism and homeland security information. The implementation of any one or more of these approaches will have a net positive impact on FBI information sharing with SLT agencies regardless of the election or failure to implement any of the other

approaches. The implementation of the approaches examined in this thesis is the next logical step to enable the FBI to substantially improve FBI information sharing with SLT agencies started 9 years ago after the tragic events of 9/11.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

9/11 Commission	National Commission on Terrorist Attacks Upon the United States
AGG-DOM	United States Attorney General Guidelines for Domestic Operations of the Federal Bureau of Investigation
BRU	Blanket Routine Uses
CRS	FBI Central Records System
DCIS	Defense Criminal Investigative Service
DHS	Department of Homeland Security
DI	FBI Directorate of Intelligence
DOJ	Department of Justice
ECPA	Electronic Communications Privacy Act
FBI	Federal Bureau of Investigation
FIG	FBI Field Intelligence Group
FISA	Foreign Intelligence Surveillance Act
GAO	U.S. Government Accountability Office
IA	Intelligence Analyst
IB	Intelligence Bulletin
IIR	Intelligence Information Report
IRTPA	Intelligence Reform and Terrorism Prevention Act of 2004
ISE	Information Sharing Environment
JTTF	Joint Terrorism Task Force
LEO	Law Enforcement Online
N-DEx	National Data Exchange
NCIC	National Crime Information Center
NCTC	National Counterterrorism Center
NISS	National Information Sharing Strategy
NSI	National Suspicious Activity Reports Initiative
PII	Personally Identifiable Information
PM-ISE	Program Manager–Information Sharing Environment

RFPA	Right to Financial Privacy Act
RISS	Regional Information Sharing System
SA	Special Agent
SAR	Suspicious Activity Reports
SIR	Situational Intelligence Report
SLT	State, Local and Tribal
TFO	Task Force Officer
TIDE	Terrorist Identities Datamart Environment
TSC	Terrorism Screening Center
TSDB	Terrorist Screening Database
USG	United States Government
USIC	United States Intelligence Community
VGTOF	Violent Gangs and Terrorist Offenders File
WMD Commission	Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction
XML	Extensible Markup Language

ACKNOWLEDGMENTS

This thesis is dedicated to my dad, Pedro “Pete” Gomez, who lost his battle with cancer shortly after I was accepted into this program. He and my mom, Joan, taught me through word and deed that I could be professionally and personally successful by living and working with integrity and compassion. I also must acknowledge the love and support of my wife, Joanne, who supported me throughout this 18-month program. She was always understanding and supportive during my trips out to Monterey and countless weekends and evenings when I was physically home, but mentally in the CHDS world researching, reading books and articles, writing papers and this thesis or posting to Moodle.

I also wish to acknowledge the support and incredible skill of my colleagues and friends in the Boston FBI and Joint Terrorism Task Force (JTTF), especially Squad CT-1. It has been an honor to be their colleague and friend for the past 12 years. Their dedication and skill has made us all safer. I am humbled and always challenged to supervise this exceptional group of federal, state and local agency personnel fighting the terrorist threat in New England and around the world. I especially want to recognize SAC Warren Bamford (retired), who always generously supported me personally, professionally and academically. I also received unwavering support from everyone on Squad CT-1, especially Jamie and Andy, who did their job and mine during all my trips to Monterey.

I was very fortunate to have the support and expertise of Dr. Robert Josefek and Dr. Ed Valla throughout the thesis process. They were always generous with their time and expertise, including their incredible ability to nudge me in the right direction to find the best answer or approach on my own. Your contributions have dramatically improved this thesis and me.

I must recognize the visionaries in the Center for Homeland Defense and Security (CHDS) and the FBI University Education Program (UEP), who created these incredible

programs that merge academic rigor from a group of incredibly impressive and generous faculty and staff with the practical experience of the impressive cadre of homeland security professionals throughout the country to make up Cohort 0901/0902 and the alumni. I am humbled to have been afforded this fantastic opportunity to expand my horizons in their company. I look forward to many years of making my small contribution to the academic and operational world of homeland security in their company.

The 18 months in this program and 12 years working on the JTTF in Boston have taught me that we must pursue homeland security together as "one team, one fight."[1] I hope this thesis can contribute in some small way to the continued expansion of the homeland security team and improve the effectiveness of the fight. In the world of homeland security, our sum is certainly greater than our individual parts.

[1] "One Team, One Fight" is the motto of the FBI National Joint Terrorism Task Force (JTTF).

I. INTRODUCTION

A. PROBLEM STATEMENT

Since 1980, the Federal Bureau of Investigation (FBI) has been investigating terrorism threats to the United States through Joint Terrorism Task Forces (JTTF), which now have more than 4,400 members from over 600 state, local and tribal agencies (SLT) and 50 federal agencies at 106 locations across the United States (FBI, n.d. (b)). Although the JTTFs are new, the FBI has been engaged in investigating terrorism since at least the 1920s. The FBI began investigating terrorism cases and threats in the 1920s with the Palmer Raids and Wall Street bombings (FBI, n.d. (k)). Although the exact volume of information collected by the FBI during these decades of investigating terrorism matters is classified, the thousands of investigators must have generated an enormous volume of terrorism information of intelligence value. Some of this information could be helpful to other agencies to enhance national security and prevent future terrorist attacks.

Two major commissions concluded that information sharing is crucial for preventing another terrorist attack and protecting the United States. This view is also widely held by not only the president, but also most others in the national command structure of the U.S. government. The caveat in all the information sharing Congressional Acts, Presidential Orders and Executive Branch policies and plans is a variation of the requirement for the information sharing while ensuring the protection of all privacy, civil liberties and other legal rights. In the 9 years since the 9/11 attacks, the federal government and SLTs have developed numerous "ad hoc" information sharing arrangements, but there still is not an effective and systematic method for information sharing. The Markle Foundation Task Force on National Security in the Information Age (Markle Foundation Task Force) described the criticality of information sharing in their March 2009 report:

> The 9/11 Commission identified ten lost "operational opportunities" to derail the 9/11 attacks—and most involved a failure to share information. Progress on information sharing is the single most important step required to improve the national security of the United States. If there is another terrorist attack on the United States, the American people will neither

> understand nor forgive a failure to have connected the dots. Lack of progress on information sharing is a clear and present danger to the country. (p. 3)

1. Obstacles to Information Sharing

FBI information sharing is significantly restricted by regulations and policies created to ensure compliance with the Privacy Act of 1974. This act mandates that "No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency . . . unless disclosure of the record" was with the consent of the individual or meets 1 of 12 exceptions, including the exception permitting the information to be shared with other members of the agency with a "need for the record in the performance of their duties" (5 U.S.C. § 552a(b)). These Privacy Act restrictions apply to personally identifiable information (PII) (5 U.S.C. § 552a(a)(4)). The Privacy Act defines an individual as any U.S. citizen or lawful permanent resident alien (i.e., a U.S. Person) (5 U.S.C. § 552a(a)(2)). The primary exception permitting sharing PII in an information sharing is the "routine use" exception, which allows agencies to share PII in certain routine circumstances necessary for performance of the agency mission that are announced to the public.

2. "Ad Hoc" FBI Relationships for Information Sharing

In addition to the Privacy Act prohibitions, the FBI faces many technological limitations and obstacles that complicate information sharing. The FBI currently uses numerous "ad hoc" terrorism and homeland security information sharing relationships for to overcome the lack of an established and effective technological information sharing environment. The FBI shares all requested terrorism information, excluding domestic terrorism information, with the National Counterterrorism Center (NCTC). One of the primary "ad hoc" operational information sharing methods for the FBI with other federal agencies and SLTs is the Joint Terrorism Task Force (JTTF). The FBI Directorate of Intelligence (DI) and the Field Intelligence Groups (FIG) are primarily responsible for the production and dissemination of FBI intelligence to law enforcement and the United States Intelligence Community (USIC). The FIG maintains "ad hoc" sharing

relationships with state Fusion Centers and USAI Regional Intelligence Centers. The FBI also directly submits terrorism-related PII to three terrorism-related databases for watchlisting: Terrorism Identities Datamart Environment (TIDE), Terrorism Screening Database (TSDB), and the National Crime Information Center (NCIC) Violent Gangs and Terrorist Offenders File (VGTOF).

3. Distinction Between Intelligence and Information

Information is a necessary precursor to intelligence; however, information is not transformed into intelligence until value is added through analysis. The FBI defines intelligence on its public Internet Web site as "information that has been analyzed and refined so that it is useful to policymakers in making decisions— specifically, decisions about potential threats to our national security" (FBI, n.d. (g)). The sharing of information is critical to allow the FBI and other agencies to conduct the thorough and accurate analysis required to produce valuable intelligence. This thesis seeks to address the problem of FBI information sharing as part of this intelligence process, but does not seek to address any issues related to conducting or sharing finalized intelligence. Enhanced, expanded FBI information sharing should have an overall positive impact on intelligence at all levels of government. Finally, mechanisms created to communicate information could also effectively share intelligence products with agencies outside the FBI and USIC.

B. RESEARCH QUESTION

What are the best policy and technology available to enable the FBI to more effectively share terrorism and homeland security information maintained in FBI Case Management systems without violating privacy and civil liberty protections, including the Privacy Act of 1974?

C. SIGNIFICANCE OF RESEARCH

This research contributes to the existing literature on information sharing by recommending the utilization of existing technologies and proposing new policy

approaches to expand the FBI sharing of terrorism and homeland security related information maintained in FBI case management systems. The two-phase policy options analysis rating methodology in this thesis provides a flexible framework for future analysis of information sharing technologies and policies for any organization. The FBI will be the primary beneficiary of this research, which will be able to use this research, methodology and analysis to evaluate three different alternatives and combinations to enhance the existing "ad hoc" FBI information sharing. Ultimately, the entire homeland security community and leadership can utilize the methodology, the technology and the policies from this research to expand information sharing throughout the homeland security community. Finally, the FBI implementation of any or several of the information sharing alternatives from this research would greatly expand FBI information sharing, which would improve the FBI information sharing compliance with the numerous information sharing mandates from the president, the Congress, the attorney general and the director of the FBI. This enhanced terrorism and homeland security information sharing will also significantly contribute to the overall mission for the entire homeland security community to protect the U.S. from the terrorist threat.

D. CHAPTER OVERVIEW

Chapter II is the literature review for this thesis, examining the amount of information shared, privacy protected, security and trust. The analysis and proposals of commissions and task forces, the government and the scholars are addressed for these issues. The role and significance of the FBI in the sharing of terrorism and homeland security are also addressed.

Chapter III provides a detailed explanation of the policy options methodology utilized in this thesis. The limitations of this methodology and analysis are addressed. The chapter describes both phases of the analysis to determine the effectiveness of the information sharing approach and the feasibility of implementation of the approach. The standards for rating the effectiveness factors and criteria and the implementation factors are defined in this chapter.

Chapter IV examines the current FBI information sharing "status quo" mandated by executive orders and legislation. Specifically, numerous "ad hoc" policies and technologies developed, deployed and utilized by the FBI, since the attacks on 9/11 are addressed.

Chapter V presents the three options examined by this thesis: a new homeland security "routine use" exception, the Discoverability of Information and the XML Segregation of Information. This chapter examines the capabilities and requirements of each of these approaches, including the technology requirements.

Chapter VI analyzes all four approaches utilizing the evaluation factors developed from the literature review and the writer's experience: Information Shared, Privacy Protection, Security and Implementation. This analysis examines the criteria for each evaluation factor, which is then rated as low, medium or high. Finally, the chapter provides the overall analysis of all the approaches utilizing the rating approach described in Chapter III.

Chapter VII presents the conclusions and recommendation developed from the analysis, and addresses the benefits of implementation of the approaches in a comprehensive manner.

THIS PAGE INTENTIONALLY LEFT BLANK

II. LITERATURE REVIEW

Information sharing has been an issue of interest and concern for the Federal government and other organizations for years. However, the events of 9/11 escalated the federal government concerns over information sharing from one of many to one of the primary homeland security concerns. This increased concern for information sharing generated a significant increase in publications on information sharing and related issues. A review revealed that the literature over the past 9 years can be generally broken into the following three categories: (1) Task Force and Independent Commission Reports; (2) Government Publications and Statements; and (3) Scholarly Journals. This literature review will examine how each of these categories of literature addresses the following critical information sharing aspects: (1) Importance of Information Sharing, (2) Privacy and Civil Liberties, and (3) Security.

A. IMPORTANCE OF INFORMATION SHARING

"Information sharing is a critical activity for almost every institution" (Hexmoor, 2006, p. 130). Prior to 9/11, information sharing was an issue of concern for a wide variety of organizations, including businesses, governments and others. The attacks on 9/11 transformed information sharing from one of many issues for organizations into a critical, priority issue for all levels of government. The consensus of all three categories of literature was that government information sharing was ineffective prior to 9/11. The National Commission on Terrorist Attacks Upon the United States (9/11 Commission) concluded that information sharing was not a priority for the federal government before the attacks (9/11 Commission, 2004, p. 328). The 9/11 Commission illustrated this ineffectiveness with their discussion of the impact of the Department of Justice "wall" procedures that were misunderstood and misapplied by the FBI prior to 9/11 (9/11 Commission, 2004, pp. 78–80). However, the 9/11 Commission warned that the often-characterized problems of "watchlisting," "information sharing" and "connecting the dots" were too narrow of a focus (9/11 Commission, 2004, p. 400). The Markle Task Force and The Commission on the Intelligence Capabilities of the United States

Regarding Weapons of Mass Destruction (WMD Commission) also found deficiencies in information sharing, and the need for continued improvement of information sharing. The Markle Task Force produced its first information sharing report in 2002. The WMD Commission dedicated an entire chapter on information sharing in its final report. These three independent entities relied heavily on one another and created specific recommendations to address the identified information sharing deficiencies.

The first U.S. government efforts to address information sharing began in October 2001 when Congress passed the USA Patriot Act, with a mandate to ensure that there was no "wall" between criminal investigations and intelligence operations; and the creation of the Office of Homeland Security to integrate information and expand information sharing with Presidential Executive Order 13228 (GAO, 2006, p. 13). These actions were the first official U.S. government determinations that expanded information sharing was necessary to improve homeland security. The U.S. government continually and repeatedly asserted that information sharing is critical to national security in the more than 8 years of Congressional Acts, Presidential Executive Orders, Government Accountability Office (GAO) Reports, National Strategies and executive speeches. The GAO identified five Presidential Executive Orders and one Homeland Security Presidential Directive (HSPD), which demonstrated the importance of information sharing and mandated changes to improve information sharing. This GAO report also cited three Congressional Acts recognizing the importance of information sharing and mandating actions to improve information sharing (2006, pp. 9–13). The U.S. government published the National Homeland Security Strategy in 2002, which "identified information sharing as a foundational element in protecting from, preventing, and responding to potential acts of terrorism" (GAO, 2006, p. 9). The GAO published six reports addressing the critical nature of information sharing in homeland security, which ultimately led to their determination that information sharing was a "government-wide high risk area" (2006, p. 9). In October 2007, the administration of President George W. Bush demonstrated the criticality of information sharing with the publication of the *National Information Sharing Strategy (NISS)*, which dealt exclusively with information sharing issues more than 6 years after the 9/11 attacks. The United States

Intelligence Community (USIC) launched more than 100 initiatives to improve information sharing in the 3½ years following 9/11 (WMD Commission, 2005, p. 430). Numerous speeches by prominent members of the Executive Branch of the U.S. government expressed their personal and their agency's opinion of the critical role of information sharing in protecting the United States from future terrorist attacks. There were no significant contradictory views regarding the critical nature of information sharing in any of the government orders, publications or speeches.

Many of the significant scholarly works also recognized the critical nature of information sharing in homeland security. Professor William Pelfrey identified information sharing and collaboration as the two most important aspects of prevention, which is critical to the overall preparedness (Pelfrey, 2005, p. 9). Professor Pelfrey quoted Michael O'Hanlon from the Bookings Institute for the proposition that "the challenge of interdicting terrorists before they can act centers around the effective mobilization of information" (Pelfrey, 2005, p. 9). A common theme in the academic literature was agreement regarding the importance of information sharing for homeland security and other law enforcement functions (Bajaj, 2007, p. 29). Scholarly works also explored the importance of information sharing in the context of other organizational relationships, including financial joint ventures. However, the inherent differences in the nature of the relationships among commercial organizations from relationships amongst governmental organizations mitigated the relevance of these works to homeland security information sharing.

B. PRIVACY AND CIVIL LIBERTIES

Almost every work addressing information sharing dedicated significant attention to the issue of protection of privacy and civil liberties. This issue was the significant concern for many of the independent commissions, federal government actions, publications and statements, and scholarly works.

The WMD Commission recognized the importance of privacy protection at the beginning of the civil liberties section of its information sharing chapter with the assertion that "[n]o discussion of information sharing initiatives would be complete

without noting that the sharing of information has raised privacy and civil liberties concerns in the wake of September 11" (WMD Commission, 2005, p. 445). The Markle Task Force dealt extensively with privacy and civil liberties protections throughout all of their reports over the past 9 years. The 9/11 Commission also addressed civil liberties and privacy in their information sharing section with three specific recommendations to protect civil liberties. The 9/11 Commission quoted the Markle Task Force for their core proposition that it was critical to protect civil liberties and privacy to ensure public trust, which was essential for any effective information sharing effort (9/11 Commission, 2004, p. 419). The WMD Commission also cited the Markle Task Force for the importance of protecting privacy and civil liberties.

Despite this constant endorsement of the protection of civil liberties and privacy by these government actions and publications, they never provided specific, meaningful guidance for the actual implementation of information-sharing plans with appropriate civil liberties and privacy protections, including useful metrics. They each mandated or endorsed maximum information sharing with strict adherence to all civil liberties and privacy protections mandated by law. The Information Sharing Environment (ISE), mandated by the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) and corresponding Presidential Orders, published Privacy Guidelines and Privacy Implementation manuals on these significant issues. However, the complex nature of the civil liberty and privacy protections from federal, state and local laws and policies made defining or comprehensively understanding privacy protection an almost insurmountable obstacle, which resulted in the delegation of the responsibility for defining and implementing these protections to the lowest government levels with the greatest familiarity of their own privacy and civil liberty issues, laws and policies.

The scholarly publications also dealt extensively with the issues of privacy and civil liberties protections in homeland security information activities. The RAND Corporation examined the history of domestic intelligence in the United States, which created or exacerbated many civil liberty and privacy concerns. RAND devoted an entire section of the report *Reorganizing U.S. Domestic Intelligence: Assessing the Options* on protection of privacy and civil liberties (Treverton, 2008). Professors Liu and Chetal

acknowledged the importance of privacy protection "utilizing three subcategories: (a1) trust third party techniques, (a2) secure multi-party computation, and (a3) application specific techniques" (2005, p. 287). A significant amount of the academic literature examined the legal aspects associated with privacy concerns related to information management, utilization and sharing. Professor Kasper examines the difficult-to-define concept of privacy, especially its continuing evolution, including after the events of 9/11. Professor Kasper criticized the existing privacy literature for too specifically or broadly defining privacy based on specific topics, allowing cultural bias in the definition and the value-driven nature of these works (2005). Professor Nelson examined the impact of technology and the events of 9/11 on privacy by examining the constitutional foundations for privacy and the public policy debate generated by the events of 9/11 on the issue of privacy (2004). The Heritage Foundation identified the potential of anonymization in their article about government use of commercial databases as a method to maintain privacy, while utilizing a necessary tool (Dempsey, 2004). Overall, the scholarly works had extensive concerns over the privacy issues, but generally did not limit themselves to the context of terrorism and homeland security information sharing.

C. SECURITY

Security concerns were addressed in all three categories of works, but in far less detail than the issues of information sharing and privacy and civil liberties. Security was frequently addressed as a reason for failures prior to 9/11 or a necessary requirement for effective information sharing. The related issue of over-classification was frequently addressed as a significant obstacle to information sharing with SLTs, due to the limited number of individuals with security clearances and the limited number of communication and computer systems capable of storing and transmitting classified information.

The independent commissions and task force addressed the issue of security in a limited manner, primarily as an information sharing obstacle. However, they recognized the need to protect certain information for reasons beyond privacy and civil liberties. The WMD Commission recommended assigning a high-level government official under the Director of National Intelligence (DNI) with responsibility for the information sharing

and the correlated protection through implementation of necessary security, including limitations on sharing. The 9/11 Commission recognized the need for protecting information and the "need to know" standard, but criticized the existing system, which was created for the Cold War and relied on individual agency rules now being applied to the terrorism threat (2004, p. 417). The 9/11 Commission did not make specific recommendations for security, since it primarily focused on expanded information sharing to enable more effective all-source analysis to address the terrorism threat. The Markle Task Force primarily addressed security in the context of protecting civil liberties, while ensuring necessary access to information by appropriate personnel based on their role and need for information.

Due to the unique nature of individual agency issues and the sensitivity of security to the particular agency, the U.S. government addressed security issues in more general and generic ways in strategies, publications, memorandums and speeches. As an example, the ISE provided a detailed business plans to deal with protecting the information shared through their environment in the *ISE Implementation Plan*. The GAO addressed information sharing security issues, especially related to the complication of the sharing process created by the 56 different sensitive but unclassified information restrictions inhibit the ability to expansively share information (2006, p. 21). President Obama, in his *Memorandum for the Heads of Executive Departments and Agencies on Classified Controlled Unclassified Information*, recently re-addressed is vast array of sensitive but unclassified classifications. Earlier, President George W. Bush attempted to address this issue in his 2005 presidential memorandum (Obama, 2009). Both administrations mandated a prompt remedy to this problem.

The scholarly works recognized the issue of security, but primarily addressed it either as a necessary component of or a significant obstacle to information sharing. These scholarly works dealt with the technical issues associated with sharing and proposed alternatives or addressed the issue of trust as a necessary element of security and information sharing. Professors Liu and Chetal proposed an information sharing approach based on an interest-based trust model, since they believed the current trust models were inadequate (2005, pp. 286–287). Hexmoor explored the concept of "soft

security" for information sharing instead of the current "hard security" (2006, p. 128). Both of these works extensively addressed the issue of trust related to security for enhanced information sharing. Most of the other scholarly works either dealt with very specific security technology issues or the concept of security in information sharing.

D. TRUST

Trust is defined as ''a psychological state comprising the intention to accept vulnerability based on positive expectations regarding the intentions or behavior of others, irrespective of ability to monitor or control that other party" (Zolin, Hinds, Fruchter, & Levitt, 2004, p. 3). Trust is a well-established area with extensive scholarly study and publications dealing with all major aspects of trust. Numerous works in all three categories addressed the issue of trust. The Markle Task Force emphasized public trust for information sharing, while the scholars primarily explored the issue of trust in the context of security or information sharing failures. Reinhard Bachmann and Akbar Zaheer's edited volume *Handbook on Trust Research* (2006), dealt extensively with traditional trust issues, including interpersonal, group and inter-organizational trust. Analysis of the current information sharing systems with SLTs by the commissions and scholarly works revealed significant reliance on trust due to the lack of any systematic method for information sharing, like the system proposed by the president, Congress, the Markle Task Force, and others related to information sharing.

Professors Cook, Hardin and Levi examined the issue of trust in *Cooperation Without Trust?* (2005). They utilized the encapsulated interest model of trust, which considers the interests of the trusted party as perceived by the trusting party. Under this model, trust exists when the trusting party believes that the trusted party's interests are consistent or compatible with their interests on a particular issue or interaction (2005, pp. 5–8). They cite a declining level of trust in society due to the increasing complexity of society and reduced reliance on trust in routine relationships. Instead, they proposed to "motivate cooperativeness through manifold devices" (2005, p. 197). This work is particularly relevant to the relatively new field of homeland security, since it is likely

that information sharing will take place in homeland security relationships with trust, lack of trust, and possibly affirmative distrust.

The particular academic definition of trust either focused on psychological state and intention or on actual actions or rational interests, had a great influence on the perception of the necessity of trust in information sharing. Trust is critical in the decision to share information and determining the appropriate extent of information sharing; however, the decision to share has already been made by the president and U.S. Congress. Therefore, the existence trust, distrust or a lack of trust may influence the scope of sharing by particular individuals or organizations, but it will not change the fundamental decision to share.

E. FBI INFORMATION SHARING

As mentioned above, the FBI's JTTFs throughout the country investigate terrorism threats inside the United States. The information generated from these investigations would be valuable to SLT homeland security agencies. This role and the vast amount of terrorism and homeland security information in FBI systems make the FBI a crucial participant in any meaningful information sharing effort.

The 9/11 Commission rejected the idea of an American "MI-5"[2] and provided a long list of recommendations for improvement of the FBI, including enhanced information sharing utilizing the existing JTTFs (2004, pp. 423–425). The Markle Foundation Task Force described the FBI, as "the agency responsible for collecting intelligence on terrorists in the U.S. . . . the only U.S. domestic intelligence agency" (2003, p. 95). The WMD Commission dedicated an entire chapter to the Department of Justice (DOJ), FBI and Department of Homeland Security (DHS) addressing concerns regarding all of these critical participants in homeland security. The 9/11 and WMD Commissions both addressed the historical shortcomings of information sharing prior to 9/11, the efforts to improve the FBI and the need for additional improvements in the future.

[2] MI-5 is the United Kingdom domestic intelligence agency also known as the British Security Service.

Numerous government publications addressed the role of the FBI in information sharing and plans for improving this information sharing. The FBI expressed its information sharing strategy on their public Web site:

> The FBI's National Information Sharing Strategy (FBI NISS) ensures that information is shared as fully and appropriately as possible with SLT partners in the intelligence and law enforcement communities. The FBI NISS is based on the principle that FBI information technology (IT) systems must be designed to ensure that those protecting the public have the information they need to take action. It also ensures that information is shared within the bounds of the Constitution. (FBI, n.d. (e), ¶ 1)

The GAO also discussed the FBI's role in information sharing, including sharing information through the JTTFs (2006). The *National Information Sharing Strategy (NISS)* discussed changes to the FBI and its critical role in future information sharing. Executive Orders, Congressional Acts, strategies, speeches and other documents also came to a consensus that the FBI has a critical role in information sharing.

As part of the DOJ Law Enforcement Information Sharing Plan (LEISP), the FBI utilizes numerous technologies to implement their information sharing efforts, including Law Enforcement Online (LEO), eGuardian, Regional Information Sharing Systems (RISS) and the National Data Exchange (N-DEx) with SLTs. "LEO is a 24-hours-a-day, 7-days-a-week, on-line, controlled-access communications and information-sharing data repository" (DOJ-OIG, 2007, p. 26) enabling the sharing of law enforcement, terrorism or other information on a secure network accessible from the Internet anywhere in the world. eGuardian is a FBI computer system for reporting Suspicious Activity Reports (SAR) through Fusion Centers to the JTTFs for further investigation or analysis. SARs can be submitted or reviewed by SLTs and federal law enforcement agencies by accessing eGuardian through LEO (FBI, 2008 September 19). eGuardian has been incorporated as the FBI component of the Shared Space utilized for the National SAR Initiative (NSI) implemented as part of the Information Sharing Environment (PM-ISE, 2009, pp. 18–19). RISS is a DOJ information sharing system accessible through LEO and other computer systems to facilitate sharing criminal intelligence that complies with Federal Regulation 28 CFR Part 23 (RISS, n.d.). N-DEx is a new computer system

being developed and implemented by the FBI to allow federal and SLT law enforcement systems to share criminal information. N-DEx will enable these agencies to identify previously unknown connections between entities or places utilizing information in N-DEx maintained by the other law enforcement agencies participating in N-DEx (FBI, 2008 April 21).

The role of the FBI in information sharing was not a primary focus of the scholarly works, which focused more on the macro issues of security, privacy and national security. Michael O'Hanlon expressed his view that in "any prevention-based information strategy, the FBI will be crucial. It is a core agency in collecting information about potential terrorists, a focal point for collating and analysis, and—as a law enforcement agency—an essential user of information" (O'Hanlon, 2002, p. 13). The other scholarly works did not focus significant attention on the FBI's role beyond examining the historical failures of the FBI and other agencies prior to the attacks. Their primary focus was creating the capacity to share information throughout the federal, SLTs and private entities to protect homeland security.

F. CONCLUSION

Many works from a variety of government and non-governmental sources, including independent commissions and task forces, federal government sources and scholarly works, examined pre-9/11 information sharing failures by the FBI, intelligence and military organizations. A review of the literature showed no work, which disputed the value of information sharing, but they all recognized the importance of protecting privacy and civil liberties. Despite this recognition, none of these works provided a comprehensive analysis of these privacy limitations. In most instances, this responsibility was delegated to those implementing the information sharing efforts and the owners of the underlying information. Information security was addressed to a much lesser extent, but was recognized as a potential significant impediment to effective information sharing.

Trust was cited frequently as a vital aspect of information sharing related to other issues, like protecting civil liberties and privacy or security. Although trust plays a

critical role in the current “ad hoc” sharing efforts and will likely play a role in future information sharing, the overall decision to trust SLTs with expanded information sharing has already been unequivocally endorsed by the president, the Congress and other prominent members of the U.S. Executive Branch. The current role of trust in information sharing and the well-established nature of the field of study on trust significantly reduced the need for further examination of this issue in the homeland security information sharing.

It is clear from the available literature that the FBI must play a prominent role in future information sharing efforts. Many of the works focused less on the roles of specific entities and instead on specific recommendations or comprehensive approaches to information sharing. The FBI has repeatedly asserted its commitment to information sharing, but the available information indicates that the primary focus on this effort will continue to be primarily dependant on “ad hoc” methods, like the JTTF, FIG and Fusion Centers. Unfortunately, these “ad hoc” methods are susceptible to obstructive behavior by individual FBI employees, who may be opposed to sharing information, overly protective of information or other obstructionist motivations. The FBI is developing improved technologies, including: eGaurdian, Law Enforcement Online (LEO), Regional Information Sharing System (RISS) and N-DEx. The overall field of information sharing related to homeland security has been extensively explored; nevertheless, there is still a need for work on the implementation of a systematic information sharing approach at particular agencies to accomplish the national information sharing strategies and mandates.

THIS PAGE INTENTIONALLY LEFT BLANK

III. METHODOLOGY

A. POLICY OPTIONS ANALYSIS APPROACH

This thesis will utilize Policy Options analysis to assess several policy and technology options for improving FBI terrorism and homeland security information sharing with SLT homeland security agencies. The analysis will be divided into two distinct phases. The first phase will analyze the probable effectiveness of the four approaches utilizing the following effectiveness factors and criteria identified from the literature review and writer's experience (Table 1).

Table 1. Effectiveness Factors and Criteria

Information Shared	**Privacy Protection**	**Security**
Relevance	Public Perception	Sensitive/ Classified Info
Accuracy	Privacy Act Compliance	Access Control
Timeliness	Privacy Impact Assessment	Compliance/Audit

The literature review revealed that these three effectiveness factors and their corresponding criteria are all critical for all information sharing systems. Failure to accomplish any individual effectiveness factor would result in the failure of the overall system or approach. The three criteria for each effectiveness factors are also all required for any effective information sharing system or approach. The failure of any of these criteria would likely result in the overall failure of the corresponding effectiveness factor, which would result in the failure of the system or approach. The critical nature of all the effectiveness factors and their corresponding criteria resulted in them all essentially being of equal importance in the overall assessment of the effectiveness of an information sharing system or approach. Therefore, each of the effectiveness factors and criteria were equally weighted in this analysis.

The criteria for each effectiveness factor will be rated as low, medium or high based on their anticipated performance. The definitions of low, medium and high performance for each individual criterion were created from the literature review and the writer's 12 years of experience as a FBI Special Agent and Supervisory Special Agent on the Boston Division Joint Terrorism Task Force (JTTF). The detailed description of the standards for rating each criterion will be addressed in later sections of this chapter. The ratings will be converted into a numerical value with each criterion given 1 point for a low rating, 2 points for a medium rating and 3 points for a high rating. A higher overall score indicates that the particular information sharing approach is a better option than approaches with lower overall scores.

The second phase of analysis examines four significant factors that are necessary for the successful implementation of any information sharing system or approach. These factors will not determine the effectiveness of the approach or system, but they will influence the probability of successful implementation of the particular approach or system in the FBI. The following implementation factors were identified from the literature review and the writer's experience: cultural resistance, fiscal performance, utilization of technology and training. These implementation evaluation factors will also be analyzed utilizing an equal weighting. These factors will be rated in the same manner as the effectiveness factor criteria.

B. LIMITATIONS OF ANALYSIS

Analysis of FBI information sharing is necessarily a qualitative instead of quantitative process, since the FBI does not currently quantitatively report the amount of terrorism and homeland security information that is collected, shared or withheld for privacy protection or other reasons. This limitation prevents the writer from effectively measuring the amount of terrorism and homeland security information or data in terms of characters, pages, documents or gigabytes in FBI information systems. The FBI currently does not have an effective means for measuring and publicly reporting the amount of information or data shared with SLT agencies. Furthermore, the unpredictability of the

amount and type of terrorism and homeland security information likely to be collected in the future prevents this analysis from projecting future effectiveness.

Surveys were considered as an alternative quantitative measurement tool, but they are also significantly limited in their effectiveness as a measurement tool for actual FBI information sharing. They can measure the perception of information sharing, but they do not measure the actual effectiveness and amount of information shared in the current or proposed approaches. This measurement tool is also limited by the fact that there are a relatively limited number of persons with extensive knowledge of the type and amount of information collected and maintained by the FBI and a corresponding knowledge of the information needs of the SLT homeland security agencies. The largest identifiable groups meeting all of these criteria are current and former JTTF TFOs, which were surveyed by the Department of Justice Office of Inspector General (DOJ-OIG) in 2004 to assess their satisfaction with information sharing and other JTTF-related issues.[3]

These significant measurement limitations require this analysis to examine each of the options based on the potential for information sharing, rather than actual or projected information shared. The analysis will generally assume that users and agencies will follow the policies and procedures to ensure the maximum information sharing permitted in the particular approach or technology, unless otherwise noted. Therefore, the analysis of these options represent the potential for information sharing, while the actual implementation of information sharing for any of these approaches will be dependant on the implementation factors from the second phase analysis and the actual implementation of any of these approaches by the FBI.

C. EFFECTIVENESS FACTORS AND CRITERIA STANDARDS

Phase one analyzes the effectiveness factors criteria addressed in the following sections of this chapter. These criteria will be rated to determine the overall effectiveness of each approach for the particular factor and overall.

[3] Some of the survey results appear later in this chapter of the thesis

1. Information Shared

The literature review revealed and common sense dictates that the amount and quality of information actually shared is a critical evaluation factor for determining the effectiveness of any information sharing system or approach. This effectiveness factor will be analyzed utilizing the following equally weighted criteria: relevance, accuracy and timeliness. The FBI expressed the importance of these criteria for information sharing in the *FBI NISS* vision statement asserting, "The FBI is committed to sharing *timely, relevant, and actionable* [emphasis added] intelligence to the widest appropriate audience" (FBI, 2008, ¶ 2).

a. Relevance

It is critical for any information sharing approach to provide relevant terrorism and homeland security information to the recipient. However, it is difficult to identify what is currently relevant and what will be relevant in the future for every recipient or potential recipient. The other critical aspect of this criterion is to minimize the irrelevant information that is provided, which could obscure relevant information or confuse the recipient.

b. Accuracy

Inaccurate, relevant information is of extremely limited value, since it creates a greater risk of erroneous actions or decisions. The literature review identified accuracy as another critical element for any information sharing approach or system. Traditional intelligence and investigative techniques have certain inherent accuracy and reliability issues, since the information may be obtained covertly from individuals or organizations attempting to conceal that information. Therefore, information for purposes of this information sharing analysis is "accurate" when it correctly communicates the information contained in the FBI systems, regardless of the underlying reliability of the information.

c. Timeliness

The final important criterion for assessing the information shared is timeliness. Relevant, accurate information may have no value when it is not received in a timely manner.

d. Standards for Rating Information Shared

The effectiveness for the criteria will be rated as low, medium or high based on the following scale (Table 2).

Table 2. Description of Standards for Ratings of Information Shared Effectiveness Evaluation Criteria

Evaluation Criteria	Low	Medium	High
Relevance	Can locate some relevant and exclude some irrelevant information, but can not rely on the results for action	Can locate significant amount of relevant and exclude significant amount of irrelevant information	Can locate most of relevant, while excluding most irrelevant information
Accuracy	Information discovered is accurate with significant concerns regarding completeness	Information accurately reflects significant amount of information in FBI systems. Information may be somewhat dated or limited.	Information accurately reflects the most important information in FBI systems at time of sharing
Timeliness	Significant delay in locating and obtaining information, including being highly dependent on a manual process.	Able to identify information in a relatively quick manner in close proximity to time needed. May be delay in getting the actual information.	Quickly access the information when needed

2. Privacy Protection

The literature review demonstrated the critical nature of ensuring maximum privacy protection for any information sharing system. Shared information and privacy protection are at opposite ends of the same spectrum, with the balance between these two ends critical for information sharing systems. Privacy protection is the second critical effectiveness factor, which will be analyzed and rated utilizing the following criteria: public perception, adherence to the Privacy Act and Privacy Impact Assessments (PIA). The FBI recognized the critical importance of privacy protection in the *FBI NISS* guiding principle for information sharing, which asserted:

> The FBI adheres to both Attorney General and DNI guidelines for information sharing, ensuring that intelligence and law enforcement information is shared with relevant partners while *protecting sensitive information and the privacy and civil liberties of US persons* [emphasis added] . . . Share information within the framework of US laws, DOJ LEISP Privacy Policy, and ISE Privacy Guidelines, *ensuring the FBI protects privacy rights and civil liberties of US persons* [emphasis added]. (FBI, 2008, ¶ 5 & 6)

a. Public Perception

Public perception is critical with potential for a significant impact on the privacy protection effectiveness factor in any information sharing system. A negative public perception can easily lead to the abandonment of any information or data exploitation approach, like the $54 million Total Information Awareness (TIA) "data mining" system proposed by DoD to identify terrorists operating in the United States after 9/11. "By September 2003, the hysteria against TIA had reached a fevered pitch and Congress ended the research project entirely, before learning the technology's potential and without a single 'privacy violation' ever having been committed" (MacDonald, 2004, ¶6). After TIA, privacy advocates turned their attention to Computer Assisted Passenger Prescreening System (CAPS II), a Transportation Security Agency (TSA) tool designed to confirm identities and pre-screen passengers on flights. These groups were successful again, which led to re-engineering of the project after a review ordered by DHS Secretary

Tom Ridge in July 2004. This ultimately led to a more limited $100 million pre-screening system named “Secure Flight” (Sternstein, 2004).

These two high-profile episodes illustrate the potential detrimental impact of a perceived negative privacy effect on any homeland security information technology approach. Public perceptions represent a significant risk to any FBI technological information sharing approach, and could result in a mandate for significant re-engineering or abandonment of any proposal. The FBI Investigative Data Warehouse (IDW) system also was subject to attacks based on privacy concerns, but this FBI system survived attacks by privacy advocacy groups and Congressional inquiries (Electronic Frontier Foundation, 2009). IDW, originally developed under the name Secure Collaboration Operational Prototype Environment (SCOPE), stored more than 1 billion government records from numerous federal government sources by its completion in 2005 (DOJ-OIG, 2007, p. 25). The writer reviewed the circumstances surrounding and factors involved in the termination of TIA and CAPS II compared with the successful completion and implementation of IDW in an effort to determine why IDW survived privacy based attacks, while TIA and CAPS II were destroyed or damaged by similar attacks. Unfortunately, this examination only confirmed the complex nature of public perception and its impact on systems or approaches that impact privacy in the United States. There was also public criticism of the potential privacy invasion from the FBI eGaurdian SAR reporting system, but those public criticisms have not led to a significant negative public perception against the little-known system officially launched by the FBI (Nojeim, 2009). It is nearly impossible to accurately predict when opponents to a system will be successful at generating negative public perception, which could ultimately damage or destroy the proposed system. Numerous factors can play a significant role influencing this public perception; however, there are too many intangibles to reliably predict public perception. Therefore, public perception will be impossible to analyze reliably in this thesis.

b. Privacy Act Compliance

The U.S. Congress created the Privacy Act of 1974 to protect PII information of U.S. Persons maintained in any federal government system of records. This Act is one of the primary privacy protection means for U.S. Persons. It would be politically and legally impossible to create an information sharing system or approach that violated the Privacy Act; however, the human element involved in all information sharing systems or processes creates potential for violations when there are insufficient controls or oversight. This potential for individuals to violate the Privacy Act and related policies and procedures is the focus of analysis for this factor.

c. Privacy Impact Assessment (PIA)

The E-Government Act of 2002 Section 208 mandates the federal government to conduct Privacy Impact Assessments (PIA) for all new or proposed information systems involved in the collection, storage or dissemination of PII (Public Law 107-347). DOJ mandates the creation of a PIA utilizing their standard form published on the agency public Internet Web site. A review of the DOJ PIA template and guidance revealed that the most relevant section to assess information sharing with outside agencies is Section 5 (U.S. DOJ, n.d. (c)). The existing "status quo" approach does not have a single PIA for all of them, but several of the newer components have PIAs available on the FBI public Internet site. The writer created PIA Section 5 utilizing the DOJ PIA template for each of the approaches, and evaluated them against the existing FBI PIAs utilizing criterion in the next section (FBI (n.d. (i)).

d. Standards for Rating Privacy Protection

The effectiveness for the criteria will be rated as low, medium or high based on the following scale (Table 3).

Table 3. Descriptions of Ratings Standards for Privacy Protection Effectiveness Factor Criteria

Criteria	Low	Medium	High
Public Perceptions	Members of the general public have significant concerns about privacy, and perceive the system or approach as a significant privacy threat	Members of the general public perceive the system to be concerned about privacy and take some appropriate measures to protect individual privacy. However, they perceive some risk of privacy violations.	Members of the general public perceive the system to take all necessary and appropriate measures to protect individual privacy.
Privacy Act Compliance	Complies with Privacy Act with substantial possibility of violations.	Complies with the Privacy Act with some possibility of violations.	Complies with the Privacy Act with minimal possibility of violations.
Privacy Impact Assessment	Privacy Impact Assessment completed with many sections inadequately addressed.	Privacy Impact Assessment completed with many sections adequately addressed.	Privacy Impact Assessment completed with all sections adequately addressed.

3. Security

Security is a vital aspect of any information system. Security is the final critical evaluation factor analyzed to assess the overall effectiveness of each system or approach. Security inhibits the amount of information shared, which is necessary to ensure the willingness and ability of the information owner to share their information. Security is also critical for assuring the public that privacy will be fully protected. The *FBI NISS* and DOJ LEISP both recognized the essential role of security in all information sharing. This was clearly expressed by the *FBI NISS* vision statement:

> The FBI is required to effectively balance the need to effectively and *securely share information with its responsibility to protect sources*,

> *investigative operations, national security information*, [emphasis added] and the privacy and civil liberties of US persons. (FBI, 2008, ¶ 2)

The following criteria will be analyzed to rate the effectiveness of security for each of the approaches: handling of classified/sensitive information, access control and compliance/auditing.

a. Federal Information Security Management Act of 2002 (FISMA)

The E-Government of 2002 Act, Title III, also known as the Federal Information Security Management Act of 2002 (FISMA), "requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source" (NIST, n.d., ¶ 1). Compliance with FISMA was not analyzed, since the DOJ requires all computer systems to comply with all FISMA requirements. Therefore, any approach utilizing a computer system that does not comply with FISMA would not be permissible regardless of the other capabilities of that system.

b. Handling of Sensitive and Classified Information

FBI counterterrorism reporting almost always contains classified and sensitive information comingled with unclassified information. The FBI uses paragraph marking to document the highest level of classified information in each paragraph in a document. It is impossible to differentiate which portions of the paragraph are actually classified, and to what level. Under the current system, an FBI Original Classifying Authority (OCA) is the only person permitted to officially determine the level of classification for any portion(s) of a classified paragraph. The OCA has the authority to either de-classify the entire paragraph or redact appropriate portions of the paragraph to make it unclassified.

The FBI collects and maintains a large variety of unclassified sensitive information that also **must** be protected from unauthorized disclosure mandated by numerous current statutes, rules and policies. The categories of sensitive information and

handling requirements continually change over time. The FBI **must** comply with all restrictions on all classified and sensitive information obtained or maintained in FBI terrorism and homeland security-related investigations. These restrictions are frequently created and modified by agencies and officials outside the FBI. These statutory, regulatory and policy mandates to protect the variety of classified and sensitive information make this an essential effectiveness evaluation criterion for security. Even infrequent, intermittent violations could destroy a system or prevent its development or deployment.

c. Access Control

There is inherent risk in granting access to any information or information system, which must be addressed in any information sharing system. It is vital for any information sharing approach to grant access only to those with a legitimate need for the information, while protecting information from unauthorized users. This is one of the core security issues for all existing and future government computer systems, which makes it a critical criterion for the security effectiveness factor.

d. Compliance and Audits

The last integral security aspect is assurance that sharing and withholding classified information is conducted appropriately only with authorized users for a legitimate purpose. Robust auditing capabilities allow for effective compliance review of all policies and procedures. This review is easier to conduct in an electronic system, but is still possible for a manual information sharing approach to have robust auditing to ensure compliance.

e. Standards for Rating Security

The effectiveness for the criteria will be rated as low, medium or high based on the following scale (Table 4).

Table 4. Description of Ratings Standards for Security Effectiveness Factor Criteria

Criteria	Low	Medium	High
Sensitive/ Classified Info	Significant risk of unauthorized access or disclosure of Sensitive/Classified Information	Some possibility of unauthorized access or disclosure of Sensitive/Classified Information	Sensitive/Classified Information is fully protected from unauthorized access or disclosure.
Access Control	Substantial risk that unauthorized individuals will get access to information	Some risk that individuals will get access to system or information without proper authorization	Reliable method to ensure only individuals with authorized access can obtain access to system/approach
Compliance/ Audit	No meaningful system to review access to system or information. Low probability of identifying violations. Minimal or no ability to enforce rule violations. Limited or no ability to investigate possible violations.	Some capability to review access to system or information. A reasonable probability that violations will be identified. Some means to enforce rule violations and investigate potential violations.	Substantial and reliable methods to review access to system or information. Substantial probability violations will be identified. Meaningful means to enforce and investigate violations.

D. IMPLEMENTATION EVALUATION

The second phase of analysis will examine the likelihood of successful implementation of any system or approach determined to be effective in phase one. Research for this thesis, and the writer's experience, identified the following critical factors for determining the likelihood that the FBI could successfully implement an information sharing system or approach: cultural barriers, fiscal performance, utilization of technology and training requirements. A failure or low rating for any one or more of these factors will complicate the process of implementation; however, it will not

necessarily preclude the implementation of the particular system or approach. The FBI can overcome complications associated with these factors by dedicating additional resources and effort to overcome poor performance or failure of these factors. Despite the ability to overcome these factors, the analysis of these factors is still critical to the overall evaluation of every system or approach to accurately assess the likely FBI resources and effort required for successful implementation.

1. Cultural Barriers

Organizational structure is the key values, guiding beliefs, understandings, symbols, rituals and myths of an organization. Culture is critical and defines an organization. It is the "glue that holds organizations together" (Hennessey, 1998, p. 525). The FBI has been a law enforcement agency for more than 100 years, and has developed a distinctive culture. This culture has evolved over time with significant influences from numerous transformations and generations of employees. After the attacks of 9/11, many FBI critics focused on the need to change FBI culture, or used FBI culture as justification for creating a domestic security or intelligence agency in the United States. Director Mueller told the National Press Club in Washington, DC "'FBI culture' is the ethic of hard work, integrity, excellence and dedication to protecting the American public, all within the confines of the Constitution. I see this culture every day, in every FBI office, and in every FBI employee" (Mueller III, 2003, ¶ 26). The *FBI NISS* expressly recognized the importance of information sharing and the need to create a culture of sharing at all levels in the FBI with the following guiding principle:

> [f]oster a *culture of sharing* [emphasis added] both within the FBI and between the FBI and its federal, state, local, and tribal partners. Encourage information sharing and integration— fusing "all crimes with national security implications" with "all hazards" information. (FBI, 2008, ¶ 6)

FBI culture is difficult to define, and is subject to different interpretations by different groups and individuals inside and outside the FBI. It has been recognized that there may be multiple different cultures within an organization (Hennessey, 1998, p. 525). It was not feasible to conduct surveys or interviews to comprehensively and effectively identify the elements of FBI culture for this thesis. Therefore, this thesis will evaluate cultural

resistance and barriers to these new proposed approaches primarily by considering the severity of the change required for the new approach and the utilization of technology to mitigate potential resistance to this change. If the change is consistent with existing FBI culture, then some, many or most of the 30,000 FBI employees should embrace the proposed change. The impossibility of predicting the reaction of over 30,000 employees and TFOs makes evaluating and measuring the likelihood of acceptance extremely difficult.

2. Fiscal Performance

The FBI had a negative, expensive experience with the development of the Virtual Case File (VCF) case management system, the original Automated Case Support (ACS) replacement. The failure to deploy this system cost the taxpayers more than $100 million (Mueller III, 2005). This experience made the FBI more sensitive to the potential for a failed system and its corresponding financial and operational losses. The development and identification of a thorough and accurate estimate of the expenses of any computer system or approach is difficult an early stage of consideration. This analysis will assess the costs of these approaches in generic terms of minimal, significant or substantial. The FBI currently spends $451 million to develop and deploy Sentinel (DOJ-OIG, 2009, p. 8), spent over $12 million developing, deploying and upgrading the FBI's Threat Tracking system Guardian 2.0 and has already spent over $137 million on the development and testing of N-DEx, with more than an additional $101 million projected expenditure to complete this system as planned by the Fall of 2010 (U.S. DOJ, 2010).[4] This history of large expenditures for computer systems was the frame of reference utilized to judge the potential expenses and proportional savings from each of the proposed approaches. For purposes of this analysis, any approach that costs less than the $12 million (cost of Guardian) would be assessed to have no significant costs, anything between $12 million and $250 million (total cost of N-DEx) would be assessed as significant and anything above $250 million would be assessed as substantial costs.

[4] Expenses for Guardian and N-DEx are procurement expenses and not total expenses associated with the system, including FBI personnel costs, while the DOJ-OIG expenses contains these additional personnel expenses.

3. Utilization of Technology

The FBI recognized the importance of integrating modern information technology in the *FBI NISS*, which identified information technology as their second primary objective (FBI, 2008). The DOJ LEISP and IRTPA of 2004 also recognized the critical role of information technology in information sharing approaches. Technology is critical to the creation and implementation of all FBI terrorism and homeland security information sharing approaches. The FBI specifically addressed the critical role of technology in the following *FBI NISS* guiding principle:

> Leverage existing platforms and develop new technology to enhance our information sharing capabilities. *Continue to adopt new technology and invest in IT infrastructure* [emphasis added] that are compliant with federal standards, meet FBI needs, provide auditable information integrity and quality, provide the appropriate level of security, and allow for strong community user identification and authentication. (FBI, 2008, ¶ 6)

4. Training Requirements

The final critical factor for evaluating the implementation of any system is the training requirements. Training is critical to minimize negative impact of cultural barriers and ensure appropriate and effective utilization of technology. Inadequate training could be a significant barrier to successfully improving information sharing. Training demands are critical due to the large number of non-FBI employees, including SLT representatives from over 18,000 law enforcement and homeland security agencies, with a significant role in these approaches and extremely limited ability to be personally trained by FBI. The FBI asserted the importance of training in implementation of enhanced information sharing in the *FBI NISS* recognition that "education and training on information sharing will be widely available and required by both new and current FBI personnel" (FBI, 2008, ¶ 7).

5. Standards for Rating Implementation Factors

The following standards will be utilized to rate each of the critical implementation factors (Table 5).

Table 5. Description of Standards for Ratings of Implementation Factors

Factors	Low	Medium	High
Cultural Barriers	Approach or system is in conflict with the culture and there is no technological solution to minimize or eliminate conflict.	Approach or system is not in conflict with the culture. There are either minimal significant cultural obstacles or technology minimizes significant cultural obstacles.	Approach or system is supported by the culture or designed to be successful independent of cultural barriers.
Fiscal Performance	There are substantial financial costs associated with this system or approach.	There are some significant financial costs or minimal savings for this system or approach.	There are no significant financial costs or a substantial savings for this system or approach.
Utilization of Technology	Extremely limited or no use of technology. Primarily a manual process.	Technology plays a role in the system or approach; however, it is limited in its capability, upgradability or compatibility with other systems. Manual process may still be required in critical portions of information sharing process.	Modern and flexible technology is utilized in system or approach for enhanced performance.
Training Requirements	Substantial training required for user or FBI to utilize system or approach.	Some training required for user or FBI to utilize system or approach.	Minimal or no training is required for user or FBI to utilize system or approach.

IV. CURRENT FBI INFORMATION SHARING

In response to the numerous government mandates after the 9/11 attacks, the FBI has enhanced terrorism and homeland security information sharing with the USIC, federal and SLT homeland security agencies. This process created a complex interrelationship between systems and processes that developed in an "ad hoc" manner over these years.

A. INFORMATION MAINTAINED BY FBI

The FBI currently operates unclassified, Secret and Top Secret/Sensitive Compartmented Information (TS/SCI) computer networks to facilitate storage and communication of information, including terrorism and homeland security information. The primary network used by the FBI is a Secret network connected to the USIC, homeland security and Department of Defense (DoD) through the DoD Secret Internet Protocol Router Network (SIPRNET) (Bald, 2005). The FBI classified and unclassified terrorism and homeland security information and intelligence are stored on this Secret network, including the Automated Case Support (ACS) and Sentinel case management systems.

1. FBI Reporting Documents

The FBI primarily documents information collected in national security and other investigations in FD-302s, Electronic Communications (EC) and FD-1023s. The FD-302 and EC are currently created in WordPerfect utilizing a macro. The reporting SA, TFO or IA enters the information contained in these reports into a free-form format with the different types of sensitive and classified information comingled with minimal markings.[5] The FD-1023 is a new form for documenting Confidential Human Source (CHS) reporting utilizing a XML format document, which is created and viewed with Microsoft's InfoPath software. This form segregates some information, but the substance

[5] Examples of these documents and their markings are contained in the Appendix.

of the reporting and a significant amount of comingled sensitive and classified information is still primarily embedded in a single section of this XML document. These documents are stored electronically in the FBI's ACS case management system, which is being replaced by Sentinel (described in greater detail below).

These free-form FBI reporting documents with sensitive and classified information comingled significantly complicate the ability of the FBI to effectively share information beyond the FBI, especially with SLT homeland security agencies. The FBI does not currently have the technology either to extricate or anonymize the sensitive and classified information in these documents, which would be required to enable automated, electronic information sharing. These forms and other technology issues limit the FBI to "ad hoc" manual methods of information sharing that require an individual SA, TFO or IA to manually review documents and redact the sensitive or classified information from the document, or to create a new document, without the sensitive or classified information, that is suitable for sharing with the particular individual or group that needs the information.

B. FBI CASE MANAGEMENT SYSTEMS

The FBI Privacy Act official system of records is the FBI Central Records System (CRS), which includes the paper files maintained in all the FBI Field Offices. The majority of FBI information and intelligence is electronically stored in the FBI case management system.

1. Automated Case Support (ACS)

The Automated Case Support (ACS) computer system was created in 1995 to allow for electronic storage of FBI case documents utilizing "universal serialization" accessible to FBI personnel throughout the world on the FBI Secret computer network (Fine, 2002). ACS is a "green screen" environment that requires the user to utilize function keys instead of the modern graphical user interface environment (GUI), a.k.a.

mouse, commonly used on most modern computer systems (Higgins, 2002).[6] The DOJ OIG conducted numerous audits of ACS, and concluded that ACS "uses outmoded technology, is cumbersome to operate, and does not provide necessary workflow and information-sharing functions" (DOJ-OIG, 2008, p. vi). The FBI unsuccessfully attempted to replace ACS with Virtual Case File (VCF), which failed and was abandoned by the FBI in 2005. This eventually led to the new FBI Case Management system, Sentinel, currently under development (Mueller III, 2005).

ACS has built-in text search capabilities to locate terrorism and homeland security information. Additionally, SAs, TFOs, IAs and others can also search this information stored in ACS through the FBI Investigative Data Warehouse (IDW), which contains multiple other data sets and a more effective search capability than ACS (Mueller III, 2005). In 2006, FBI Assistant Director John Miller responded to a critical *Newsweek* article with the following description of the capabilities of IDW and ACS in counter terrorism investigations:

> Investigative Data Warehouse, a computer system developed in-house, with off-the-shelf software connects over a billion counter terrorism records, and the Automated Case Support System, cross indexing everything from a major suspect to an obscure name found on the back of scrap-paper in an Afghan cave to a suspicious financial transaction report filed with the Treasury Department. It also searches across data in forty other federal agencies to "connect the dots." These tools and others, developed since 9/11, available to agents and analysts across the country and around the world, have helped thwart a number of terrorist plots in the U.S. over the past five [5] years. In fact, just in the past year, terrorist plans in Torrance, Calif., Atlanta, New York, Washington, Miami, and Toledo, Ohio, were detected and disrupted. The FBI also played a key role in the interdiction of plots in the U.K, Canada, Bosnia and a number of places that cannot be disclosed because operations continue. (¶ 2)

The FBI is currently transitioning to a new case management system, Sentinel, which is described in greater detail in the following section. The FBI FD-302s and ECs

[6] "Green screen" refers to the earliest computer systems that were incapable of displaying color and required all commands to be typed on the keyboard. This refers to the earliest commercial computer systems and the original personal computers from the 1980s.

are still created in free-form documents uploaded into ACS. The FBI is currently developing new XML forms to replace the existing FD-302 and EC in Sentinel.

2. Sentinel

Designed by Lockheed Martin, Sentinel is a Web-based case management system designed to handle all FBI investigations and intelligence operations. Phase One of this program was delivered in June 2007 with significant portions of Phase two delivered in the summer of 2009. The FBI expects final delivery of Sentinel in the summer of 2010 (Mueller III, 2008). Director Mueller informed the House Judiciary Committee that Sentinel was "one of our [the FBI's] most important programs" (Mueller III, 2009, ¶ 17). Sentinel is a program with integrated commercial off-the-shelf (COTS) components. Sentinel will have electronic information management, automated workflow processes, search capabilities, and information sharing capabilities with other federal, state, local and tribal law enforcement agencies and the USIC (DOJ-OIG, 2008, p. 1). FBI Director Mueller expects Sentinel to utilize XML documents to facilitate enhanced information sharing capacity (Mueller III, 2005). The FBI recently experienced complications with the development and deployment of Sentinel, which led the FBI to report a delay in completion until an unspecified date in 2011, and a revised estimated cost above the expected $451 million (DOJ-OIG, 2010, p. 2).

C. PRIVACY ACT LIMITATIONS

FBI information sharing is significantly restricted by FBI regulations and policies designed to ensure compliance with the Privacy Act of 1974. The Privacy Act mandates that "No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency . . . unless disclosure of the record" was with the consent of the individual or meets 1 of 12 exceptions, including an exception that permits the information to be shared with other members of the agency with a "need for the record in the performance of their duties" (5 U.S.C. § 552a(b)). The Privacy Act restrictions apply to personally identifiable information (PII), which is defined as "any item, collection, or grouping of information about an individual that is

maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph" (5 U.S.C. § 552a(a)(4)). The Privacy Act defines an individual as any U.S. citizen or lawful permanent resident alien (i.e., a U.S. Person) (5 U.S.C. § 552a(a)(2)). The primary exception permitting expansive sharing of PII is the "routine use" exception. The "routine use" exception permits an agency to share Privacy Act records for any purpose compatible with the original purpose for collection in accordance with a "routine use" published in the Federal Register. Numerous other statutes and rules also impose restrictions upon information collected by sensitive sources or means, including Federal Rule of Criminal Procedure 6(e), Right to Financial Privacy Act (RFPA), Electronic Communications Privacy Act (ECPA), Foreign Intelligence Surveillance Act (FISA) and others.

The FBI promulgated policies to apply all the necessary restrictions to FBI Privacy Act Systems of Record, including the FBI Central Records System (CRS). The FBI CRS Systems of Records Notice (SORN) was published in the Federal Register, as required by the Privacy Act. The FBI published fifteen Privacy Act Blanket Routine Use (BRU) exceptions applicable to the CRS (FBI, n.d. (d)). BRU-1 authorizes sharing a Privacy Act record when the record on its face or when combined with other information establishes a violation of law, regulation, rule, order or contract. This authorizes the record to be disclosed to an entity responsible for its enforcement, including SLTs and other federal agencies. There is a similar exception in the Privacy Act itself that allows for the sharing of this type of information with a written request of the head of the agency detailing the information needed and the criminal or civil enforcement purpose (5 U.S.C. § 552a(a)(4)). BRU-1 removes the need for the FBI to get this written request from the head of the agency. BRU-6 permits disclosure when mandated by federal statute or treaty (FBI, n.d. (f)). The FBI added BRU-14 and BRU-15 in 2005 to permit the disclosure of Privacy Act records to SLTs for purposes related to the hiring and retention of employees and licensing. BRU-1 inhibits the sharing of FBI terrorism and homeland security information, since the majority of FBI counterterrorism investigations are

primarily intelligence investigations that do not necessarily involve an immediately apparent potential or actual criminal violation. BRU-6 is even more restrictive, since the laws, orders, regulations and policies limit the disclosure by existing privacy and other legal protections. None of the other FBI BRUs provide a lawful basis for sharing any terrorism or homeland security related Privacy Act records in a systematic and comprehensive manner. Therefore, the Privacy Act currently inhibits the FBI from providing sufficient Privacy Act records to allow for meaningful terrorism and homeland security information sharing beyond current "ad hoc" relationships. The FBI has the legal authority to unilaterally create additional "routine uses" under the Privacy Act (5 U.S.C. § 552a(e)(4)(D)). There is a certain amount of information sharing inherent in all investigations involving other agencies, including joint investigations; however, this is also conducted in an "ad hoc," limited manner, controlled by the Privacy Act.

D. FBI "AD HOC" SHARING EFFORTS

The FBI engages in numerous "ad hoc" terrorism and homeland security information sharing relationships to overcome the lack of an established and effective technological information sharing system. The FBI shares all terrorism information, excluding domestic terrorism information, requested by the National Counterterrorism Center (NCTC). NCTC is the focal point that co-locates more than 30 intelligence, military, law enforcement and homeland security networks to facilitate maximum information sharing of all terrorism information in the possession of the United States Government (USG) (NCTC, n.d.). NCTC uses this information to create finished intelligence products to share throughout the USIC. The FBI also shares information with the Interagency Threat Assessment Coordination Group (ITACG), which is made up of state and local agency members "established to develop coordinated intelligence reports and analytical products regarding terrorist threats and related issues that address the needs of state, local, tribal, and as appropriate, private sector entities" hosted at the NCTC (FBI, 2008, ¶ 27).

1. Joint Terrorism Task Force (JTTF)

The Joint Terrorism Task Force (JTTF) is the primary "ad hoc" operational means of terrorism and homeland security information sharing with other federal agencies and SLTs. Members have a top secret clearance, which grants them to access most terrorism and homeland security information in FBI files and electronic systems. JTTF liaison contacts are not required to have a security clearance, and are limited in their access to terrorism and homeland security information by their clearance level (DOJ-OIG, 2005, p. 18). The FBI shares PII with JTTF TFOs pursuant to the Privacy Act exception that allows sharing PII with agency officers and employees with a "need to know" (5 U.S.C. § 552a(b)(1)). Unfortunately, this exception does not authorize TFOs to provide the PII information to their parent agency without a separate Privacy Act exception or "routine use." This exception addresses JTTF operational necessity and permits situational awareness for the parent agency through their TFOs, which is accomplished through regular member meetings. The frequency of these meetings varies according to the situation and needs of the individual JTTF. The JTTF holds Executive Board meetings on at least a quarterly basis to facilitate information exchanges with heads of other agencies and other top-level managers from participant agencies (DOJ-OIG, 2005, p. 37). A DOJ-OIG survey of JTTF members in 2004 revealed that 77% of the respondents rated the quality of the information sharing at these meetings as Good to Excellent (DOJ-OIG, 2005, p. 32). This JTTF "ad hoc" information sharing does not facilitate significant FBI PII sharing in an expansive and effective manner beyond these informal meetings with JTTF members and their management.

For example, the case of Major Nidal Malik Hasan, the U.S. Army psychiatrist who killed 13 and wounded 33 during his attack at Fort Hood in November 2009, illustrates these current limitations on sharing information capacity with JTTF participant agencies. The FBI Baltimore JTTF conducted a threat assessment of contacts by Major Hasan with the subject of a JTTF terrorism investigation in December 2008. This threat assessment was conducted by a TFO from the Defense Criminal Investigative Service (DCIS), who concluded that these communications were consistent with research being conducted by Major Hasan at Walter Reed Medical Center. The FBI generally described

the limitations and procedures for sharing information with the JTTF TFO parent agency in the following press release related to the Major Hassan threat assessment:

> Standard protocols—based on federal law, regulations, and policy, including the Privacy and Freedom of Information Acts—govern information handling in federal task force settings, including JTTFs. JTTF-generated information may only be disseminated outside the structure of the JTTF (including to a member's home agency) with the approval of the JTTF FBI supervisor. In this case, following the review and analysis conducted by investigators, there was a conclusion made by the investigator and the supervisor that Major Hasan was not involved in terrorist activities or planning. Further dissemination of the information regarding Major Hasan was neither sought nor authorized. (FBI, 2009, November 11, ¶ 8)

2. Field Intelligence Group (FIG)

The FBI Directorate of Intelligence (DI) and the Field Intelligence Groups (FIG) are primarily responsible for FBI intelligence production and dissemination to law enforcement and USIC. The FIG maintains "ad hoc" information and intelligence sharing relationships with fusion centers and USAI regional intelligence centers with embedded SAs or IAs with on-site access to the FBI Secret computer system, including ACS and Sentinel. Access to the FBI Secret computer network at Fusion Centers enables the FBI personnel to perform their mission at the center with a secure means of classified communication. In 2007, the FBI reported a total of 256 FIG personnel, including 123 IAs, were assigned to 36 Fusion Centers across the U.S. (Mines, 2007). The DI and FIG disseminate intelligence and information through Intelligence Information Reports (IIR) ("raw intelligence") Intelligence Bulletins (IB), Situational Intelligence Reports (SIRs) and Intelligence Assessments ("finished intelligence") (FBI, n.d. (h)). The Privacy Act restricts this "ad hoc" sharing and dissemination of intelligence publications by the DI and FIG to the same standards applied to the JTTFs. FBI intelligence publications do not routinely provide PII in compliance with Privacy Act restrictions, USIC and DI requirements. Access to or utilization of FBI computer systems for Fusion Center members is governed by Privacy Act limitations and all FBI security restrictions.

3. Terrorist Watchlist Information Sharing

The FBI submits terrorism-related PII to three terrorism databases: Terrorist Identities Datamart Environment (TIDE), Terrorist Screening Database (TSDB), and the National Crime Information Center (NCIC) Violent Gangs and Terrorist Offenders File (VGTOF). This information can also be submitted to additional appropriate databases or lists, including the Transportation Security Administration (TSA) selectee or no-fly lists, the Department of State and other watchlists. Approximately 400,000 individuals are listed on the terrorist watch lists, but most are not U.S. citizens. There are approximately 3,400 people on the no-fly list, of whom approximately 170 are U.S. Persons (Healy, 2009). TIDE is a classified terrorist database maintained by NCTC with some of the derogatory terrorism information to support nominations to the Terrorist Screening Database (TSDB), which is commonly referred to as the "terrorism watchlist" maintained by the Terrorism Screening Center (TSC) (Boyle, 2007). In fiscal year 2009, the TSC had approximately 19,000 positive hits for known or suspected terrorists on the TSDB from over 55,000 "encounters" by federal and SLT agencies (Healy, 2009). TSC Director Timothy J. Healy identified the following standards for an individual being placed on the TSDB to the U.S. Senate in December 2009:

> First, the biographic information associated with a nomination must contain sufficient identifying data so that a person being screened can be matched to or disassociated from a watchlisted terrorist. Second, the facts and circumstances pertaining to the nomination must meet the "reasonable suspicion" standard of review established by terrorist screening Presidential Directives. Reasonable suspicion requires "articulable" facts which, taken together with rational inferences, reasonably warrant a determination that an individual is known or suspected to be or has been engaged in conduct constituting, in preparation for, in aid of or related to terrorism and terrorist activities, and is based on the totality of the circumstances. Due weight must be given to the reasonable inferences that a person can draw from the facts. Mere guesses or inarticulate "hunches" are not enough to constitute reasonable suspicion. (¶ 7)

However, the Attorney General Guidelines that govern all domestic FBI investigations, including counter terrorism and national security investigations, allow the FBI to conduct investigations based on less than "reasonable suspicion" utilizing limited

investigative techniques (AGG-DOM, 2008). Therefore, FBI counterterrorism threat assessments and preliminary investigations PII will not be available to the SLTs through the TSC due to the watchlisting standards mandated by HSPD 6 (Healy, 2009).

VGTOF contains PII of FBI suspected terrorists, and is accessible through the unclassified NCIC system, which is available to law enforcement agencies throughout the U.S. This information is only available to authorized users of NCIC, who are restricted from sharing this information to unauthorized individuals. These systems function as "pointer systems," providing the TSC as point of contact to arrange collaboration and information sharing between the requesting agency and the FBI. The Privacy Act limits all subsequent communications between the FBI and requesting agency.

4. The Anti-Terrorism Advisory Councils (ATAC)

Immediately following the 9/11 attacks, all 93 United States Attorneys Offices (USAO) created the Anti-Terrorism Advisory Councils (ATAC), formerly called the Anti-Terrorism Task Forces (ATTF). The U.S. Attorney General memorandum dated 9/17/2001 directed the ATTFs to "coordinate the implementation of an operational plan for preventing terrorism, serve as the conduit of information about suspected terrorists between federal and local agencies, and coordinate the district's response to a terrorist incident" (DOJ-OIG, 2005, p. 11). There were approximately 11,000 ATAC members in 2004. The DOJ-OIG distinguished the ATAC from the JTTFs, which are "primarily investigation oriented. Although the FBI field offices engage in information sharing, they meet primarily with law enforcement officials, and the information sharing is more narrowly focused than the information disseminated by the ATACs" (DOJ-OIG, 2005, p. 31). The ATACs hold monthly or quarterly meetings to facilitate information sharing. The FBI participates in these ATAC meetings as a means of information sharing beyond the members of the JTTF and law enforcement community. These meetings are limited in their level of classification by the security clearance and "need to know" of the attendee with the lowest level security clearance and least "need to know." A DOJ-OIG survey in 2004 revealed that 77% of the ATAC respondents rated the value of the information sharing in these meetings as good to excellent (DOJ-OIG, 2005, p. 32).

E. CURRENT FBI INFORMATION SHARING TECHNOLOGIES

The FBI shares information and intelligence with other agencies through multiple independent systems, including LEO, RISS, eGuardian, NSI, N-DEx, and OneDOJ. These are described in greater detail below.

1. Law Enforcement Online (LEO)

Law Enforcement Online (LEO) is a "secure, Internet-based communications portal for law enforcement, first responders, criminal justice professionals, and anti-terrorism and intelligence agencies around the globe" (FBI, n.d. (a), ¶ 3). LEO was originally created in 1995 as a dial-up system with only 20 members to facilitate enhanced collaboration and information sharing. It has expanded to over 100,000 users. LEO is accessible via the Internet through a virtual private network (VPN). LEO organizes and controls "sensitive but unclassified" information by placing that information in controlled access Special Interest Groups (SIGs). The owner of the SIG controls the type of information posted there, and grants or revokes permission to LEO users to access this information. LEO has emergency management capability with Virtual Command Center (VCC), which enables real-time information sharing and situational awareness for users granted access to the VCC for a particular threat, case or event (FBI, n.d. (a)).

The FBI operates several SIGs on LEO to share information and finished intelligence products. Intelligence products disseminated on LEO are also available through the DHS, Homeland Security Information Network (HSIN) (Bald, 2005).

2. Regional Information Sharing System (RISS)

The Regional Information Sharing System (RISS) was created by DOJ, Bureau of Justice Assistance (BJA), 30 years ago to support criminal investigations and prosecutions throughout the U.S. RISS was created and is funded to address regional crime and information sharing problems in the six RISS regions across the U.S. In 1997, RISS created RISSNET, a secure intranet system to facilitate communication and information sharing nationwide among RISS members. RISSNET contains criminal

intelligence information, which requires "reasonable suspicion" pursuant to Federal Regulation 28 CFR Part 23. RISS is accessible through LEO. RISS currently has 8,100 member agencies from federal, state, local and tribal agencies in all 50 states, the District of Columbia, U.S. territories, Australia, Canada, and England (RISS, n.d.). RISS provides access to unclassified FBI intelligence products, but it does not provide access to FBI computer systems and raw information.

3. eGuardian and National SAR Initiative (NSI)

eGuardian is a computer system designed to facilitate sharing terrorism-related suspicious activities to the JTTF through Fusion Centers in a secure, efficient, electronic manner. This system integrates with the FBI Guardian Threat Tracking system used by all FBI Field Offices to investigate unpredicated terrorism-related threats and suspicious activities. eGuardian was originally created independent of the Information Sharing Environment (ISE), which is fully integrated as the FBI component of this system. eGuardian is now fully functional and available to law enforcement agencies throughout the world on LEO. An eGuardian incident reviewed and approved by the agency and its Fusion Center is viewable by all other members of eGuardian for the duration established by the submitting agency (up to 5 years). All eGuardian incidents with a nexus or inconclusive nexus to terrorism are maintained in eGuardian with FBI disposition notes. All eGuardian incidents with no nexus to terrorism are removed from eGuardian to protect civil liberties and privacy (FBI, 2008, September 19). The FBI reports all Internet tips received from the public in the eGaurdian system for investigation by the JTTFs (FBI, 2009, June 26). Ultimately, the future of this system will be determined by its effectiveness and utilization by federal agencies and SLTs. It is important to recognize that terrorism SARs are the proverbial "searching for a needle in the haystack" approach to identifying potential terrorists. The ISE reported, in November of 2009, that approximately 1,500 incidents were submitted to eGaurdian, with only 66 of them ultimately being determined to have some probable nexus to terrorism (Black, 2009). However, given the significant potential consequences of a successful terrorist attack, every opportunity must be pursued that could result in the identification a potential terrorist.

The ISE-PM is developing a "Shared Space" concept to facilitate sharing terrorism-related information. eGuardian will be the FBI conduit to this "Shared Space." The ISE-PM created a *Concept of Operations (CONOPS)* for a National SAR Initiative (NSI) to standardize reporting of terrorism-related SARs as mandated by the *National Strategy for Information Sharing (NSIS)* released on December 23, 2008 (PM-ISE, 2008). The ISE-SARs will be accessible by fusion centers, authorized federal, SLT law enforcement agencies, DHS Headquarters, and the FBI's JTTF and FIGs to support regional and national analysis. (PM-ISE, 2008) In December 2008, the PM-ISE made a detailed announcement regarding the ISE-SAR Evaluation Environment (ISE-SAR EE) deployed to several sites to assess the technical, business practices and other aspects of the proposed NSI implementation (PM-ISE, 2008). The ISE reported, in October 2009, that the Los Angeles Police Department (LAPD) ISE-SAR EE collected over 1,900 terrorism-related SARs, with only 126 ultimately referred to the JTTF. More than 40 reported from front-line officers leading to arrests (Back, 2009).

4. Law Enforcement National Data Exchange (N-DEx)

The Law Enforcement National Data Exchange (N-DEx) is a computer system being developed by the FBI under the DOJ LEISP. It encompasses a "national information-sharing system available through a secure Internet site for law enforcement and criminal justice agencies . . . to search and analyze data using some powerful automated capabilities, helping to connect the dots between people, places, and events" (FBI, 2008, April 21, ¶ 5). The FBI expects to fully deploy N-DEx in the summer of 2010, which would make it accessible to approximately 18,000 law enforcement agencies across the country. Once fully deployed, N-DEx is expected to have the following capabilities:

- Nationwide searches from a single access point;
- Searches by "modus operandi" and for clothing, tattoos, associates, cars, etc.—linking individuals, places, and things;
- Notifications of similar investigations and suspects;
- Identification of criminal activity hotspots and crime trends;
- Threat level assessments of individuals and addresses; and
- Visualization and mapping features. (FBI, 2008, April 21, ¶ 8)

N-DEx consolidates information from all participating law enforcement agencies. These agencies share or restrict their information in N-DEx to ensure their security, privacy and other requirements. N-DEx will not contain any new information that does not already exist in other law enforcement computer systems. It will contain only criminal justice information, and not intelligence information. Information accuracy will be controlled by the contributing agency in accordance with N-DEx policy pursuant to the mandatory Memorandum of Understanding (MOU). Recipient agencies may not use or further disseminate N-DEx information without permission of the originating agency, except in exigent circumstances. N-DEx recognizes the following exigent circumstances permitting immediate action with subsequent notice to the originating agency:

> (a) there is an actual or potential threat of terrorism, immediate danger of death or serious physical injury to any person, or imminent harm to national security; and
>
> (b) it is necessary to disseminate such information without delay to any appropriate recipient for the purpose of preventing or responding to that threat. (FBI, 2007, Section 4)

5. OneDOJ

OneDOJ, also known as Regional Data Exchange (R-DEx), is a LEISP data repository of criminal controlled unclassified information (CUI) from the DOJ law enforcement components, including FBI, Drug Enforcement Administration (DEA), Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF), U.S. Marshals Service (USMS) and Federal Bureau of Prisons (BOP). The DOJ described the primary purpose of OneDOJ in their Privacy Impact Assessment (PIA) as:

> Sharing criminal law enforcement information across the Department and, secondarily, with state/local/tribal law enforcement agencies in order to more effectively investigate, disrupt, and deter criminal activity, to protect the nation's security. (U.S. DOJ, 2008, p. 1)

OneDOJ is accessed by a secure VPN over the Internet and administered by the FBI Criminal Justice Information Services (CJIS) Division in West Virginia. OneDOJ contains both structured and unstructured, free-text documents created by the DOJ law enforcement components.

An authorized OneDOJ user can conduct searches of the system data by person, place or thing. The user will be notified of the existence of a document responsive to the search, which the user can review on the system and/or request by directly contacting the contributing agency. Information obtained by a recipient user or agency from OneDOJ may not be used as the basis for any action or disseminated outside the agency without written permission from the contributing agency. This rule expressly prohibits the recipient user or agency from placing this information in an official case file or using the information in preparation of subpoenas, warrants or affidavits. An exigent circumstances exception identical to N-DEx allows the immediate dissemination or further action on the information in limited exigent circumstances (U.S. DOJ, 2008, p. 9).

OneDOJ enables the sharing of information in the system for homeland security purposes utilizing the following Privacy Act "routine use" exceptions:

> To a criminal, civil, or regulatory law enforcement authority (whether federal, state, local, territorial, tribal, or foreign) where the information is relevant to the recipient entity's law enforcement responsibilities.
>
> To a governmental entity lawfully engaged in collecting criminal law enforcement, criminal law enforcement intelligence, or national security intelligence information for law enforcement or intelligence purposes . . .
>
> In an appropriate proceeding before a court, or administrative or adjudicative body, when the Department of Justice determines that the records are arguably relevant to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding. (U.S. DOJ, 2008, pp. 9–10)[7]

[7] OneDOJ has several other Privacy Act "routine use" exceptions that are not likely to be relevant for a homeland security related use, which are omitted from this thesis.

OneDOJ is limited to authorized law enforcement personnel in participant agencies with a MOU with the DOJ. OneDOJ contains virus protection, boundary security systems and encryption to protect system data. OneDOJ maintains logs and conducts audits to ensure compliance by agencies and users with the OneDOJ rules, which can be enforced against the individual or agency. OneDOJ complies with all requirements mandated by the U.S. Congress in the Federal Information Security Management Act of 2002 (FISMA, 44 U.S.C. § 3541) (U.S. DOJ, 2008, pp. 15–18). OneDOJ is accessed through an open, XML-based, NIEM-compliant standard called LEXS-SR, which regulates the interface between OneDOJ and regional sharing systems (U.S. DOJ, n.d. (b)).

V. ALTERNATIVE POLICY OPTIONS

This thesis analyzes the existing status quo discussed in Chapter IV with the following three alternatives to improve FBI information sharing with SLT homeland security agencies: (1) a new Homeland Security "Routine Use" Exception to the Privacy Act; (2) XML Segregation of Information and (3) Discoverability of Information. This chapter provides a detailed description of these three alternatives.

A. NEW HOMELAND SECURITY "ROUTINE USE" EXCEPTION

This option addresses the legal limitations of the Privacy Act with current FBI "routine use" exceptions discussed in Chapter IV. This option is not a technology solution like the other two, but it could be utilized with either or both of the proposed technology solutions to expand the overall scope of FBI terrorism and homeland security information sharing. The FBI's current approach significantly limits terrorism and homeland security information sharing by utilizing key "routine uses" created before the 9/11 attacks or intended to address non-homeland security requirements and threats. The exact scope of permissible terrorism and homeland security information sharing under the existing "routine use" exceptions may cause confusion among FBI employees and TFOs, which creates an increased risk that some terrorism and homeland security information will not be shared by individual FBI personnel to ensure compliance with the Privacy Act, unless the investigation is a terrorism case involving clear criminal law violations. *The Attorney General Guidelines for Domestic Operations of the Federal Bureau of Investigation (AGG-DOM)* authorize investigations of threats to national security without requiring establishment of a specific violation of a federal statute. The existing "routine use" exceptions inhibit the ability to create and utilize robust technology solutions for FBI terrorism and homeland security information sharing in primarily intelligence-based investigations.

1. Process for Creating New "Routine Use"

The FBI can unilaterally modify or expand the existing "blanket routine use" exceptions by creating a new proposed "routine use" exception compatible with the purpose for which the information was originally collected, and by publishing the new proposed "routine use" exception in the Federal Register. The public and interested parties are given an opportunity to comment on the proposed "routine use" exception within 30 days. The Office of Budget and Management (OMB) is given 40 days to review and comment on the proposed "routine use" exception. The OMB determined that a "routine use" is compatible with the purpose for which it was collected when it is either "functionally equivalent" or "necessary and proper." The courts have provided different rulings, but they have not been overly restrictive (Markle Foundation Task Force, 2002, pp. 129–130).

Congress exercises its oversight authority on modifications to the "routine uses" through public hearings. However, the resulting Congressional recommendations are not binding on the proposing agency, unless Congress enacts a law addressing the new proposed "routine use." The Markle Foundation Task Force's review of the Privacy Act concluded that many agencies do not abide by Congressional advice in these circumstances, and provided the following Central Intelligence Agency (CIA) example:

> The CIA, for example, proposed one of the broadest of routine uses—one covering all of its systems of records to allow disclosure "whenever necessary or appropriate to enable the CIA to carry out its responsibilities." Congress objected to the rule as overly broad and made a series of recommendations to narrow it. The CIA ignored them, however, and published the routine use as planned. While this type of circumvention has continued for most of the Privacy Act's life, the trend very recently may be toward a slightly narrower construction of the exemption. (Markle Foundation Task Force, 2002, p. 130)

2. Proposed New FBI Homeland Security "Routine Use" Exception

The author reviewed existing FBI and other agency "routine use" exceptions to create the following proposed new FBI "blanket routine use." The following "routine

use" exception would ensure the greatest sharing of homeland security and terrorism-related information with federal and SLT homeland security agencies, while still providing substantial privacy protections:

> The FBI may share homeland security or terrorism-related personally identifiable information (PII) as a "routine use" when it is necessary to assist another agency investigating a homeland security threat or investigation to resolve that threat or investigation when the shared PII relates to individual(s) who may be a homeland security or terrorism-related threat or target.
>
> An individual may be a threat to homeland security if the FBI or any other agency has information, an allegation indicating or an articulable factual basis for the investigation that reasonably indicates the following:
>
> a. An activity constituting a federal crime or a threat to the national security has or may have occurred, is or may be occurring, or will or may occur, and the investigation may obtain information relating to the activity or the involvement or role of an individual, group, or organization in such activity.
>
> b. An individual, group, organization, entity, information, property, or activity is or may be a target of attack, victimization, acquisition, infiltration, or recruitment in connection with criminal activity in violation of federal law or a threat to the national security, and the investigation may obtain information that would help to protect against such activity or threat.
>
> The FBI may rely on the determination by the outside agency that the information is necessary and their determination that there is a sufficient factual basis for this "routine use" exception, unless the FBI has reason to believe these determinations are erroneous based on specific, reliable information in its possession.

This "routine use" exception would clearly define what is meant by terrorism and homeland security information based on federal statutes. The following definitions from existing federal statutes would be utilized to ensure clarity:

> **Terrorism Information**—Terrorism Information is defined in IRTPA Section 1016 (codified at 6 USC 485) as all information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities relating to:

- The existence, organization, capabilities, plans, intentions, vulnerabilities, means of financial or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism;
- Threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations;
- Communications of or by such groups or individuals; or
- Groups of individuals reasonably believed to be assisting or associated with such groups or individuals.

The definition includes weapons of mass destruction information.

Homeland Security Information—Homeland Security Information, as derived from the Homeland Security Act of 2002, Public Law 107-296, Section 892(f)(1) (codified at 6 USC 482(f)(1)), is defined as any information possessed by a state, local, tribal, or federal agency that:

- Relates to a threat of terrorist activity;
- Relates to the ability to prevent, interdict, or disrupt terrorist activity;
- Would improve the identification or investigation of a suspected terrorist or terrorist organization; or
- Would improve the response to a terrorist act.

This proposed "routine use" exception was created after the author could not locate a more appropriate existing or proposed "routine use" exception that would more effectively accomplish the goal of expanded terrorism and homeland security information sharing and privacy protection. The CIA "routine use" was not used, since it is too broad for a hybrid law enforcement and intelligence/domestic security agency like the FBI.

B. XML SEGREGATION OF INFORMATION

This approach will utilize technology to segregate the different types of classified and sensitive information from the other information. This will enable the most expansive information sharing possible for each potential recipient, while complying with all the policies and regulations for different types of sensitive information. Once the information is properly marked and segregated, this approach will utilize a computer

system(s) to make this information available to the widest possible audience in a secure and efficient manner. The following sections address the capabilities and limitations of existing technology available to securely, effectively and accurately segregate the different types of classified and sensitive information.

1. Extensible Markup Language (XML)

Extensible Markup Language (XML) is a W3C-endorsed meta-markup language using simple plain language tags to store data in a plain text format. The basic unit of markup (tag) and data (text) is called an element. Any program capable of reading plain text can display all the elements of a XML document. XML documents resemble Hyper Text Markup Language (HTML) documents. XML documents are not limited to a fixed set of tags like HTML documents. This flexibility allows XML tags to continually be modified to address the needs of any group or system at any particular time (Harold, 2004, pp. 3–4).

XML documents that meet the basic XML grammar rules, for example, what the tags look like and where they are placed, are said to be "well-formed." Any XML parser can read a well-formed XML document without rejecting the document. Markup describes the structure of the document, including which elements are associated with each other and what type of data can be contained in a specific element (i.e., date, name, social security number, etc). The permissible markup for an XML application can be defined in a schema, which can be in the XML document itself or in a separate document. Document Type Definition (DTD) is the schema recognized by W3C that defines all legal markups for a particular document, including where and how it can be stored in the document. These DTDs have limited capabilities, which led to the creation of numerous other schemas for expanded functionality and capabilities (Harold, 2004, pp. 3–5).

XML is only a markup language, which means that it is not a programming language, a network transport protocol or a database. However, XML has the capability to interact with software that performs these functions. For example, a Web browser can use HTTP to transmit and receive XML documents or the documents can be converted into a database like Oracle or MySQL. The capabilities and compatibility of XML make

it an excellent format for allowing different systems or programs to communicate with each other without the complication and expense of creating additional software or requiring a built-in capability to translate proprietary binary data of one program into the other. "XML offers the tantalizing possibility of truly cross-platform, long-term data formats" (Harold, 2004, p. 6).

The following is an illustration of a simple, well-formed XML (Figure 1).

```
<person>
        <name>
                <last_name> Gomez </last_name>
                <first_name> Peter </first_name>
        </name>
        <title> Supervisory Special Agent </title>
</person>
```

Figure 1. Illustration of a Well-Formed XML

2. National Information Exchange Model (NIEM)

> NIEM, the National Information Exchange Model, is a partnership of the U.S. Department of Justice and the Department of Homeland Security. It is designed to develop, disseminate and support enterprise-wide information exchange standards and processes that can enable jurisdictions to effectively share critical information in emergency situations, as well as support the day-to-day operations of agencies throughout the nation. (NIEM, n.d., ¶ 1)

NIEM is a product of Global Justice Information Sharing Initiative (Global), which expanded on their work with Global Justice XML Data Model (GJXDM) with the creation of this new standard. NIEM is a reference model, which means that organizations are not required to adopt the entire system without modification. NIEM has already been adopted by 31 states and a variety of federal and local agencies for their information-sharing initiatives (Wormeli, 2009, p. 34).

The Program Manager Information Sharing Environment (PM-ISE) utilizes NIEM for the NSI "to better enable ISE participants to share ISE-SAR information in a

standard format" (PM-ISE, 2008, p. 2). eGuardian, the FBI SAR reporting mechanism, is integrated into the NIEM-compliant NSI Evaluation Environment (PM-ISE, 2009). NIEM provides a list of standardized XML tags and rules to facilitate integration with multiple current and future homeland security systems. NIEM enables an FBI system like N-DEx to integrate with analytical commercial software, such as Coplink and Analyst Notebook, currently being used by law enforcement, military and intelligence agencies in the United States and throughout the world.

3. "Named Entity Recognition" (NER) Technology

The voluminous number of existing FBI reporting documents with comingled sensitive and classified information creates a significant problem for effective information sharing beyond current "ad hoc" methods. XML technology with appropriate policy, training and implementation will not address this problem with legacy FBI documents without the addition of some other technology or the expenditure of significant resources. One technology with potential for identifying PII in existing documents is "Name Entity Recognition" (NER), which uses computational linguistics to identify and classify words or group of words as particular entities, like persons, places or things. NER "is relatively simple and it is fairly easy to build a system with a reasonable performance, [but] there still exist many problems of ambiguity, robustness and portability, which make it difficult to attain the human performance" (Zhou & Su, 2005, p. 190). NERs are based on rules established to identify entities for the particular domain or organization. The current trend in NER is to utilize machine-learning technologies, like Hidden Markov Model (HMM), to automate the process of establishing the rules for the specific NER. Numerous different systems with both machine-learning (ML) and expert created rule-based systems (Rule) were tested by Zhou and Su for accuracy. The expert rule-based systems generally outperformed the comparable machine-learning systems. Zhou and Su conducted experiments to test the performance of different NER approaches, including their own PowerNE approach, with precision defined as "the number of the correct entity names in the answer file over the total number of the entity names in the answer file" (Zhou & Su, 2005, p. 201). The results of this testing are shown in Figure 2.

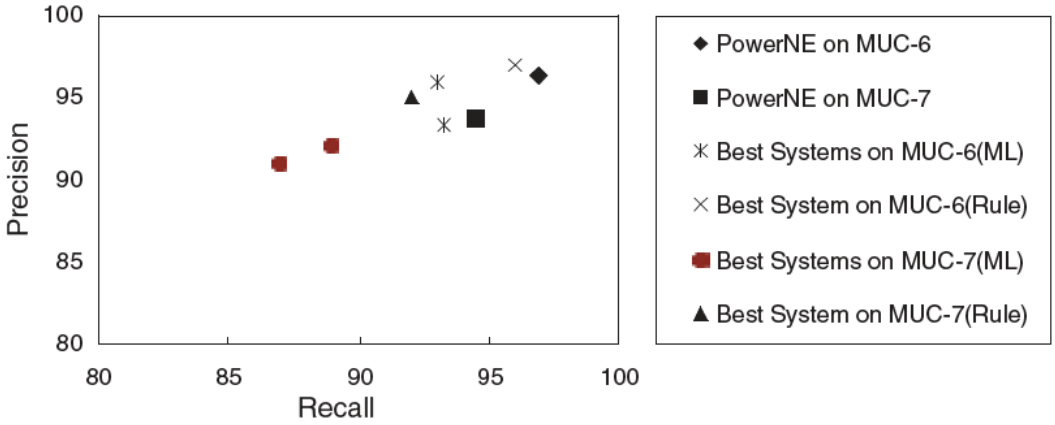


Figure 2. Comparison of Performance of NERs (From Zhou & Su, 2005, p. 202)

Unfortunately, the performance of the different NER systems ranges from approximately 85% to somewhere above 95%, which leaves some PII unidentified in documents. Therefore, the use of this technology, to tag PII for anonymization, removal or converting into a particular tag in a XML document, would not meet the legal mandates of the Privacy Act and FBI privacy policies. This technology could reduce the burden on a manual review by pre-tagging a large percentage of the PII, which would reduce the amount of PII that would need to be tagged by individuals. However, a manual review of all the FBI documents still would be necessary, and would be reduced only minimally by the use of NER technology to pre-tag potential PII.

NER technology does not address the need to remove classified information from any documents that are shared with an unclassified computer system, since the documents are marked with their overall classification and each paragraph is marked with its highest classification level. Therefore, it would need to remove the entire paragraph containing any classified information. This would also remove a great deal of valuable unclassified terrorism and homeland security information comingled in the paragraph. The fact that computers instead of an OCA conduct this process may also create problems with the FBI Security Division and classified information policies of the U.S.

government. Finally, NER and other technologies would have to be modified to identify other sensitive information to be removed. The same problem of accuracy would remain for this other sensitive information.

Based on available technology, it is highly unlikely that the FBI would be able to easily and effectively transform a significant portion of the historical unstructured data in its computer systems into a structured format like XML. However, it would still be possible to use the NER technology, especially with machine learning-based systems, to create an index of entities maintained in FBI systems with a reference to the original document. This type of Discoverability of Information approach is discussed in the next section and analyzed as one of the policy options.

C. DISCOVERABILITY OF INFORMATION

The Privacy Act, security concerns and storage of the FBI case information on a classified network significantly complicates information sharing with SLT homeland security agencies. The current "ad hoc" approaches have either a "push" or "pull" mechanism for information sharing. The originator of the information can "push" the information out to the entities the originator believes need or want the information. The "pull" approach requires the individual or agency requiring the information to affirmatively request the information from the potential information originator based on their best guess or belief that the agency has, or may have, relevant information. The intelligence process addresses this obstacle by publishing intelligence requirements that clearly express the needs of a particular agency to other members of the USIC. SLT homeland security agencies can request intelligence or information through formalized "requests for information" (RFI) or through the informal "ad hoc" relationships. The Discoverability of Information approach seeks to remedy these shortcomings by enabling authorized users to search a database or index of FBI information to determine if there is information of potential value. The information may not be directly available in this type of system, but the system allows the user to submit a request to the originator for specific information, instead of submitting a request to every agency that may have information

about the particular subject matter. This system also alleviates the burden on the FBI of conducting the search or making a determination of which recipients may need the information.

1. Markle Foundation Task Force Proposal

The Markle Foundation Task Force proposed the Systemwide Homeland Analysis and Resource Exchange (SHARE) Network, a de-centralized Discoverability of Information approach. The Markle Foundation Task Force preferred this approach over sharing all the information with every user, since that "could increase the threat to civil liberties, heighten the risk of a leak of sensitive information, cause uncoordinated action by different agencies, and simply overwhelm the recipients" (Markle Foundation Task Force, 2003, p. 12). The SHARE Network was proposed as a "peer-to-peer" system allowing "on demand" and "ad hoc" information sharing. The Markle Foundation Task Force suggested a directory to facilitate communication between and identification of subject matter experts across agency lines. They also recommended the use of XML technology, previously discussed in this chapter, to allow for identification of information of value to outside agencies through the SHARE Network. The Markle Foundation Task Force recognized the need for security, recommending the use of technologies like smart cards, information rights management and anonymization to protect sensitive information from unauthorized users or uses. They acknowledged the lack of a 100% solution to ensure security, but suggested a combination of these and other developing technologies to ensure effective security. The SHARE Network requires robust auditing with immutable logs to ensure the proper access, use and protection of information (Markle Foundation Task Force, 2003, pp. 8–17).

2. German Counter-Terrorism Database

On December 31, 2006, the Federal Republic of Germany government implemented the *Act on Setting up a Standardized Central Counter-Terrorism Database of Police Authorities and Intelligence Services of the Federal Government and the Länder (ATDG, Act on Setting up a Counter-Terrorism Database)* authorizing the

creation of a counter-terrorism database (Schäuble, n.d.). The law requires participating agencies, which include both police and intelligence agencies, to store basic information on the subjects of their investigations, and some subject contacts, for offenses of participating in or supporting an international terrorism organization, or unlawfully using or inciting the use of violence to enforce political or religious interests. The law also requires storing the same type of basic information for individuals with more than a superficial or coincidental contact with a person committing the offense or organizations, groups, foundations or businesses where there is the potential to obtain additional information for investigating and fighting international terrorism (Bundestag, 2006, p. 2). The German law requires submission of the following basic information to the counter-terrorism database:

> surname, first name, previous names, other names, aliases, divergent spellings of names, sex, date of birth, place of birth, country of birth, current and previous nationalities, current and previous addresses, special physical features, languages, dialects, photographs, name of the category pursuant to Section 2, and information on identity documents (basic data) if this does not violate other legal provisions and is necessary to identify a person. (Bundestag, 2006, p. 2)

The law also requires extended basic data for the subjects of these investigations and any contacts "aware of the planning or commission of an offence." The law requires the following additional information: telephone numbers, e-mail addresses, vehicles, banking information, special skills, religious affiliation and other relevant data (Bundestag, 2006, pp. 3–4).

The German counter-terrorism database mandates greater identifying information than the current U.S. terrorist watchlists discussed in Chapter IV. The TIDE database has the capability to maintain much of the extended data required in the German Counter-terrorism database. Unfortunately, TIDE is maintained on a highly classified computer network. VGTOF requires searches with a name and one other identifier through the unclassified NCIC network, which significantly reduces its utility in comparison to the German counter-terrorism database. The NCIC system is accessible by all the law

enforcement agencies, while the German database is limited to officials involved with counterterrorism operations at all levels in German government granted access to the database (Bundestag, 2006, p. 5).

The German counter-terrorism database has the capability to protect highly sensitive information by partially or wholly storing the extended basic information in restricted storage. There is also the capability to store all the information in "covert storage" to ensure that no one has access to even the basic information of the investigation. When a search is conducted of data in "covert storage," the agency that entered the information will be immediately notified and is obligated to determine whether they can share the information as intelligence with the searching agency (Bundestag, 2006, p. 5). VGTOF has a similar capability, but without the express requirement for subsequent contact by the originating agency to the requesting agency, for a "silent hit."

The German counter-terrorism database exemplifies a database with more than basic identifying information of subjects of an intelligence/domestic security agency that is electronically accessible by the portions of law enforcement entities working international terrorism matters in Germany. This database is relatively new and there have not been any publicly reported significant successes associated with this database.

D. TECHNOLOGY REQUIREMENTS FOR XML SEGREGATION OF INFORMATION AND DISCOVERABILITY OF INFORMATION APPROACHES

The XML Segregation of Information and Discoverability of Information approaches both require technology, including networks and software programs to prepare, securely store, effectively search and securely share appropriate information with all appropriate authorized users. The XML Segregation of Information requires a more sophisticated computer system to facilitate the actual sharing of information and protect information stored in the system. The Discoverability of Information approach requires a less sophisticated computer system with appropriate security and search capabilities, since the actual information will not be stored in the system.

Several current and developing computer systems have potential to perform the necessary functions for one or both of these approaches. The German Counter Terrorism Database described above is already designed, implemented and performing the core functions of the Discoverability of Information approach. The existing IDW system has the necessary security and robust search abilities. It currently conducts full searches and returns the full content. It may be possible to utilize a portal like the one in eGuardian to transfer information from the unclassified LEO network into the FBI Secret computer network; however, there currently is no capability to automatically return the results to the user back through a portal into the unclassified network. The FBI intends to create the capacity to transfer unclassified information from the classified FBI Guardian system on the secret network to the unclassified eGuardian system, but this capacity does not currently exist (FBI, 2008, September 19). Therefore, the current technological limitations require a manual review of the results by an authorized FBI user with access to the FBI Secret Network, who would then provide the permissible information to the outside user searching the system or at least provide a reference number (e.g., file and serial number of document). This would be a labor-intensive system that would only automate the search function and still require the involvement of a FBI entity or unit like the TSC. It may also be possible that an existing index of IDW and the IDW search capability could provide information identifying FBI document(s) (e.g., file and serial number) to allow for subsequent quick retrieval, review and sharing. This IDW search capability could be easily deployed in classified systems like SIPRNET and HSDN. Many issues need to be resolved prior to deploying any IDW-related or similar system in an unclassified computer system and network.

Of these systems, the most promising may be N-DEx, with inherent capabilities to perform the functions of both XML Segregation of Information and Discoverability of Information. This system is still under development and expected to be deployed in the Fall of 2010. N-DEx is currently intended for criminal intelligence, but the capabilities could either be expanded to address terrorism and homeland security information or as a blueprint for an identical, parallel system designed for sharing FBI terrorism and

homeland security information. The following chart, from the FBI public Internet site, illustrates the intended functioning of N-DEx for criminal intelligence (Figure 3).

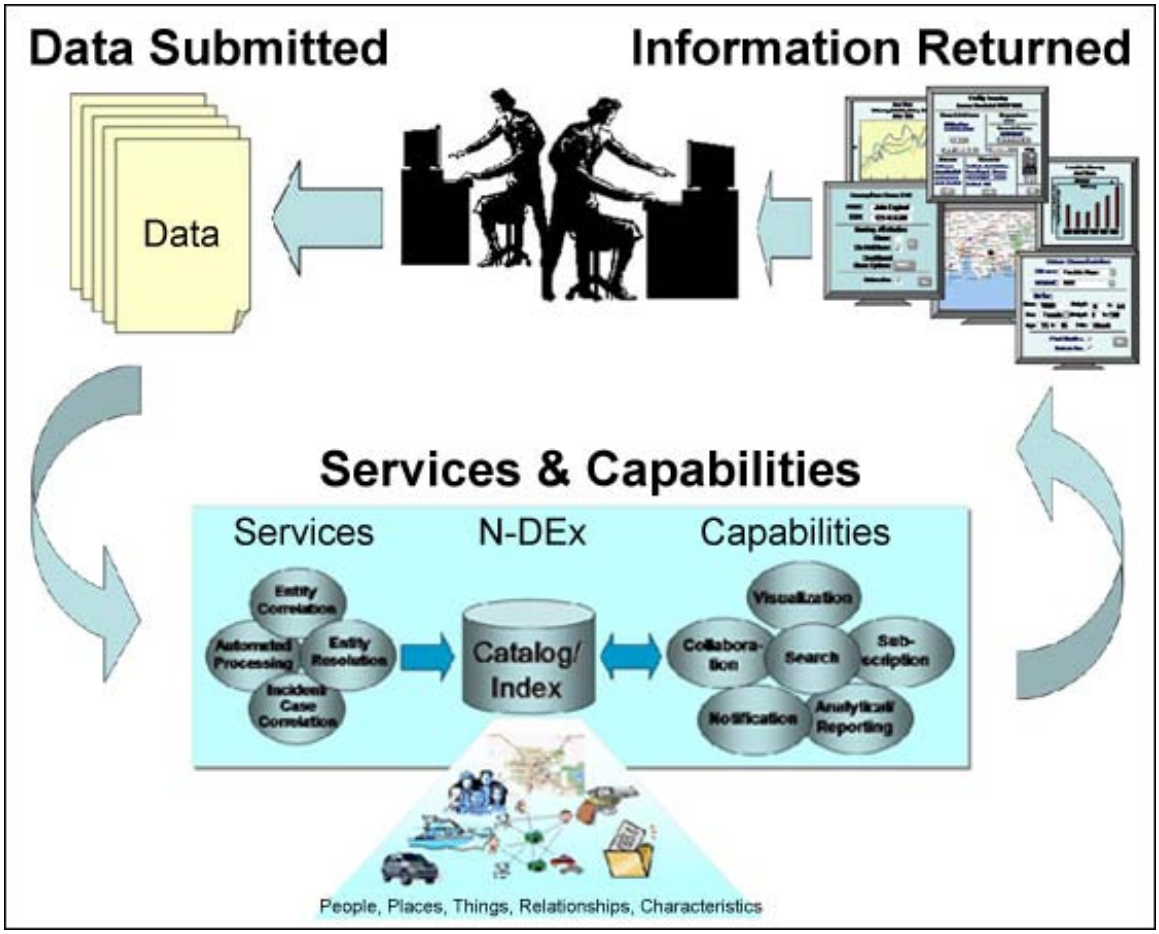


Figure 3. N-DEx Concept (From FBI, n.d. (j))

N-DEx can perform the necessary security access and restrict information in the following manners:

> **Full Access (Green)**–If the submitter of a data record (e.g., incident report, arrest report) has designated it to be fully shared, then all N-DEx users with the appropriate access authority will have access to the full record and all data elements within the record.
>
> **Pointer-Based Access (Yellow)**–If the data submitter decides that access to a specific record, or specific data elements, should be restricted except under certain circumstances, then the data submitter can designate the

> record accordingly using pointer-based sharing. With pointer-based sharing, any user that gets a “hit,” or attempts access to a record with this designation, will be provided with information on how to contact the designated record submitter (i.e., the POC for the record) only. It is then the responsibility of the data requestor to contact the data submitter who will determine whether the record can be shared. If so, N-DEx provides mechanisms so that the data submitter can make accessible that information to a specific user or group of users as applicable.
>
> **Restricted Access (Red)**–There will be circumstances where a data record or part of the record is so highly sensitive that the data contributer [sp] completely restricts access to it and to any knowledge of that record to a selected user or user group. The value of having the record in N-DEx is that the data submitter can benefit from correlations made with other N-DEx records without compromising the information contained in the sensitive record. With restricted access, any "hits" against the restricted record will be known to the submitter user/group while the submitter of the other record that it hit against will have no knowledge of the correlation. (FBI, 2007, January, Section 1(C))

The most significant obstacle to utilizing N-DEx for either of these approaches will be handling the classified information, which cannot be stored in an unclassified system. Therefore, some ability to identify this information with at least a pointer system would be critical for deploying an effective system. These issues will be examined in greater detail in the Chapter VI analysis of these approaches and systems.

Finally, these existing and developing systems could provide the foundation for creating an entirely new system to realize the requirements for the XML Segregation of Information or Discoverability of Information approaches in classified, unclassified or both environments. The FBI prefers to use these systems or other existing commercial off-the-shelf (COTS) alternatives with minor modifications compared to creating a new computer system. Additional detailed, operational capabilities and functions of the system or network are not necessary for the analysis of these options, and could be counterproductive for the development and deployment of either of these approaches.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. ANALYSIS OF INFORMATION SHARING POLICY OPTIONS

This thesis analyzes the current FBI information sharing "status quo" and the following three policy and technology options: a new homeland security "routine use" exception, a Discoverability of Information approach, and a XML Segregation of Information approach. This analysis will be conducted in two phases. The first phase examines the effectiveness of the approaches by rating them on the effectiveness factor criteria for information shared, privacy protection and security. The second phase examines the implementation of these approaches by rating the following four implementation factors: cultural resistance, fiscal performance, utilization of technology and training requirements.

A. EFFECTIVENESS EVALUATION ANALYSIS

1. Information Shared

a. Relevance

The "status quo" and proposed homeland security "routine use" exception approaches both rely on existing "ad hoc" methods of information sharing, as detailed in Chapter IV. They both depend on the FBI to identify terrorism and homeland security information relevant to a particular agency. Once the relevant information is identified, it can be manually shared through the existing mechanisms with the appropriate outside agency personnel. An outside agency can request relevant information from the FBI through an RFI or informal "ad hoc" relationships, but the requestor is completely dependent on the FBI user's ability to find the relevant information and determine that the information can be shared with the requesting outside agency. The requesting agency may or may not know that there is actually relevant or potentially relevant information in the possession of the FBI that is withheld, or the reason(s) for withholding that information.

The new homeland security "routine use" exception allows the sharing of expanded PII compared to the "status quo," which is limited by the current "routine use"

exceptions for criminal, civil and regulatory violations. The expanded scope of permissible PII sharing enables the new homeland security "routine use" approach to share a greater amount of relevant information with SLT homeland security agencies. There will not be a corresponding increase in irrelevant material, since the overall information reviewed for sharing will be the same as the "status quo" approach. The homeland security "routine use" exception ensures that all relevant terrorism and homeland security information can be shared as long as it is related to an investigation with some level of predication (i.e., suspicion or allegation of a terrorism threat). The only option permitting greater sharing of relevant terrorism and homeland security information is the previously discussed CIA "routine use" exception that permits the sharing of relevant information solely at the discretion of the CIA.

The Discoverability of Information and XML Segregation of Information approaches are technological solutions with substantial similarities. These two approaches allow the outside agency direct access to FBI information through a network, database or other technological solution. The outside agency is not dependent upon an FBI user to search FBI systems for relevant information. Instead, the outside user conducts searches of the available FBI terrorism and homeland security information to identify information that may be relevant to their investigation or threat. Both of these systems can restrict information for operational, security or legal reasons. The systems should either advise the outside agency that information is being withheld or notify the appropriate FBI of the search by the outside agency to ensure that even restricted relevant information is reviewed on a case-by-case basis for sharing with outside agencies.

The Discoverability of Information approach is a pointer system that provides a reference number (e.g., the FBI case number and serial of particular document[s]) for potentially relevant terrorism and homeland security information in the FBI system. The inability to review the actual information on a real-time basis increases the possibility of missing relevant information or requesting irrelevant information, which significantly reduces the potential for the Discoverability of Information approach to locate relevant and eliminate irrelevant information compared to the XML Segregation of Information approach.

The XML Segregation of Information approach segregates the relevant and irrelevant information, facilitating maximum sharing of relevant information to each recipient. The capability to conduct real-time searches and immediately review the maximum amount of potentially relevant information maximizes the ability of the outside agency to identify and access relevant information, while excluding or ignoring the maximum amount of irrelevant information. The security level of the system, laws and policies may limit access to this information, which requires the outside agency to use existing "ad hoc" methods with the reference information provided by the system. The XML Segregation of Information approach would provide the maximum capability of searching new FBI terrorism and homeland security information outside existing FBI computer systems, only limited by Privacy Act and security issues.

A significant limitation in the short term for the XML Segregation of Information will be handling the historical FBI terrorism and homeland security information. Since NER technology is not suitable to automatically convert the historical information into XML, the FBI will either have to conduct a manual review to tag this information or implement an index or "pointer system" like the proposed Discovery of Information approach for historical FBI terrorism and homeland security information.

These two technological approaches are currently limited to sharing relevant terrorism and homeland security information related to criminal, civil or regulatory enforcement by the "status quo" Privacy Act "routine use" exceptions. The *AGG-DOM* authorizes the FBI to conduct terrorism investigations of threats to national security regardless of evidence of criminal activity, as long as the investigation is not exclusively based on constitutionally protected behavior or profiling. A liberal interpretation of the current "routine use" exception may allow for sharing a great deal of terrorism and homeland security information, but there is still a reasonable risk that relevant information will be withheld, based on the variety of interpretations of this exception. Therefore, these two exceptions can only share the same amount of relevant information permitted under the "status quo," since neither of these approaches authorizes the sharing of additional information.

This analysis resulted in the following ratings (Table 6) for the relevance criteria, utilizing the descriptions provided in Chapter III.

Table 6. Relevance Criteria Ratings

Criteria	Status Quo	HLS Routine Use	Discoverability of Information	XML Segregation of Information
Relevance	Medium	High	Medium	Medium

b. Accuracy

The "status quo" and new homeland security "routine use" exception approaches are both dependent on the current manual communication methods for accuracy. The manual sharing process, even if the actual method of communication is technology like e-mail or telephone, creates certain inherent problems regarding accurate communication for all methods of human communication. The interpretation of the FBI employee or TFO providing the information could influence the accurate understanding of the information by the recipient. In some circumstances, it would be possible to provide a physical copy of the original information, which would significantly reduce—but not eliminate—accuracy issues. The manual sharing process also limits the ability of the recipient to easily obtain updated information to ensure access to the most updated accurate information. Ultimately, these two methods are subject to the inherent accuracy issues involved with manual sharing and communication between human beings and organizations. However, the new homeland security "routine use" exception has a greater potential to communicate the most accurate information, since it allows sharing of more relevant terrorism and homeland security information compared with the "status quo" exceptions' more limited capacity to share PII related to criminal, civil and regulatory violations.

The Discoverability of Information approach does not provide the actual information, which creates the same accuracy concerns dependent upon the method of

communication. The XML Segregation of Information approach enables the greatest level of accuracy with its immediate access to the maximum amount of permissible FBI information for the outside agency. This ability to review the actual information significantly reduces the detrimental impact of inherent accuracy issues in human and organizational communication. There may still be information unavailable directly through the system due to classification or other restrictions. The sharing of this unavailable information will have the same inherent accuracy issues in all three other approaches. Finally, the ability to easily and quickly obtain new relevant information significantly reduces any negative impact on accuracy caused by additional information that clarifies, modifies or augments understanding the original information that is subsequently added to the system.

The analysis above resulted in the following ratings for these four approaches (Table 7).

Table 7. Accuracy Criteria Ratings

Criteria	Status Quo	HLS Routine Use	Discoverability of Information	XML Segregation of Information
Accuracy	Medium	High	Medium	High

c. Timeliness

The "status quo" and new homeland security "routine use" exception approaches are significantly limited in their timeliness by the manual information sharing methods. These approaches require a FBI user to manually search FBI systems for all relevant information required by the outside agency. These approaches also require a manual process to securely communicate information to the outside agency, which produces an additional delay in the information sharing process. This dependence on manual processes of searching and sharing means the timeliness is limited by the schedule of the FBI personnel, which will result in routine information sharing generally

taking place during regular business hours. The FBI could remedy this predicament with additional personnel assigned to access the terrorism and homeland security information beyond regular business hours.

The Discoverability of Information and XML Segregation of Information approaches both provide immediate, real-time access to a computer system that enables the user to search for relevant information at any time. This real-time search capability for the Discoverability of Information approach is a significant improvement, since technology can maximize time saving associated with the initial communication and search function required for the "status quo" and new homeland security "routine use" exception approaches. The Discoverability of Information approach still requires the existing manual information sharing processes, which creates the same timeliness issues as the "status quo" and new homeland security "routine use" exception approaches. The XML Segregation of Information approach eliminates all timeliness concerns for information available through the electronic system, except for historical documents that require employing the "status quo" approach, the Discoverability of Information approach or an enormous commitment of resources to transform existing information into a suitable XML format. The information restricted in the system for all approaches would still be subject to the timeliness limitations of the existing manual information sharing processes

The analysis above resulted in the following ratings for these four approaches (Table 8).

Table 8. Timeliness Criteria Ratings

Criteria	Status Quo	HLS Routine Use	Discoverability of Information	XML Segregation of Information
Timeliness	Low	Low	Medium	High

2. Privacy Protection

a. Public Perceptions

The FBI "status quo" approach was rated as medium, since these systems have already been implemented, or are in the process of being implemented, by the FBI. The public and privacy advocates are fully aware of these systems and approaches. They have had sufficient opportunity to raise concerns to influence public perception of these approaches. Considering their history of attacking systems early in the process to prevent their continued development or deployment, the public and privacy advocates have either elected not to attack these "status quo" systems, or have failed in their efforts. Both TIA and CAPS II experienced attacks early in their creation, which ultimately led to a negative public perception and detrimental impact on funding. It is still possible there could be a change of the public perception of the "status quo" systems and approach; however, it is impossible to predict the likelihood of these situations. Overall, the current FBI "status quo" approaches and systems have not created the heightened level of public concern associated with the negative public perceptions of TIA and CAPS II.

The requirement to publish Privacy Act notices in the Federal Register for all of the new approaches, and to create and publish PIAs, ensures that the public and privacy advocates will have significant details regarding these new approaches and systems. Therefore, the other two effectiveness evaluation criteria for privacy protection will have a significant impact on public perception. The complexity and unpredictability of the factors and circumstances surrounding public perception make it nearly impossible to accurately predict the probability of both a negative public perception and detrimental action being taken against the approaches and systems.

The new homeland security "routine use" exception is unlikely to outperform the existing "status quo" approach in the public perception evaluation factor, since it seeks to expand information sharing without any corresponding improvement in control or accountability to enhance privacy protection. Therefore, the new homeland security "routine use" exception would likely achieve either a medium or low rating for public perception. The circumstances surrounding the implementation, including the

perceived terrorism threat and invasion of privacy, will be the greatest factors influencing public perception. These circumstances cannot be predicted prior to the public proposal of the system and they can substantially change during the development or deployment of this approach. The CIA Privacy Act example reported by the Markle Foundation Task Force demonstrates that the FBI could commit to the new homeland security "routine use" exception regardless of public and political opposition, which would significantly reduce the criticality of this factor.

The two technological approaches are likely to be highly susceptible to the impact of public perception, since they will require funding and authorization from political officials outside the FBI. The funding for both TIA and CAPS II were terminated by outside political and public pressure, while the FBI's IDW system survived similar attacks and scrutiny. The FBI success developing and implementing systems like IDW and eGuardian indicate there may be some factors specific to the FBI or its method of implementation that enhances their ability to mitigate or overcome potential negative public perception associated with systems or approaches that may have a negative impact on privacy. The FBI could mitigate this issue by utilizing less expensive or existing systems with only minimal modifications, which would expedite the process of implementation and reduce impact of Congressional inquiries in response to negative public perceptions.

The inherent complexity of assessing future public perception, and the ability of public perception to change during the process of developing, deploying and operating an information sharing system, makes it impossible to accurately predict public perception for a proposed approach and system. The subsequent effectiveness evaluation privacy protection factor criteria are likely to have an impact on public perception, which ensures consideration of privacy protection issues in systems or approaches despite the limitation in ability to accurately predict or evaluate public perceptions.

b. Privacy Act Compliance

The "status quo" and the new homeland security "routine use" exception approaches are both manual processes regulated by laws and FBI policies. The FBI

ensures compliance with these laws, policies and procedures through existing standard management approaches and documentation. Auditing of information sharing for these approaches requires a manual review of the physical and electronic forms documenting information sharing. The current task force environments encourage the substantial informal exchange of information, which further complicates the existing manual review and audit processes. This considerable dependence on individuals creates significant potential for individual users to share information in violation of policies, while circumventing existing review processes. Auditing all access of authorized FBI users to information to ensure compliance with information sharing policies is significantly complicated by their legitimate need to access the information, the volume of information maintained by the FBI and the substantial burden of auditing all access to information. Overall, the oversight and auditing of this manual information sharing process is one of many oversight functions performed by FBI management. This is a risk inherent with granting access to information through any information technology system.

As previously discussed, the FBI currently shares terrorism and homeland security PII with outside agencies when it establishes a violation of law, regulation, rule, order or contract. This exception clearly permits the sharing of relevant terrorism and homeland security information that relates to an act of terrorism or criminal act in support of terrorism; however, it is less clear when applied to FBI terrorism intelligence investigations without evidence of a criminal act. The lack of a criminal offense is never an issue when examining failures related to an actual or attempted terrorist attack, like the 9/11 attacks or the attack by Major Hassan on Fort Hood in 2009, since all retrospective examinations of successful terrorist attacks or attempts necessarily have a definitive criminal violation that would allow PII sharing. Unfortunately, the "ad hoc" method requires the FBI information holder to prospectively make this judgment with limited information, which creates potential for inconsistent sharing or withholding of otherwise relevant information based on erroneous or flawed interpretation and understanding of all the facts of the particular case or the limitations of the FBI Privacy Act policies and procedures. The new homeland security "routine use" exception authorizes sharing terrorism and homeland security information in any circumstance where the recipient or

the FBI have sufficient information indicating the information sharing is necessary to assist another agency investigating a homeland security threat or investigation to resolve that threat or investigation and the shared PII relates to an individual(s), who may be a homeland security or terrorism-related threat or target. Therefore, this new homeland security "routine use" exception permits greater sharing of relevant terrorism and homeland security information, while reducing confusion that could contribute to inconsistent and ineffective terrorism and homeland security information sharing.

The new homeland security "routine use" exception approach is designed to strictly comply with all Privacy Act requirements. The significant expansion of permissible information sharing for terrorism and homeland security information reduces the potential for Privacy Act violations, which reduces the impact of the less robust system for oversight, control and auditing of the information shared with outside agencies. This expanded permissible sharing should also reduce the individual FBI employee or TFO temptation to violate the Privacy Act or FBI policies over concerns or motivations beyond the scope or in conflict with these restrictions.

The Discoverability of Information and XML Segregation of Information approaches both have the capacity for robust immutable logging of access to FBI information. User agreements and MOUs would officially inhibit the user and agency from inappropriately accessing the information. This audit trail enables the FBI to monitor access to information for indications of unauthorized use of the system or information. This audit trail enables the FBI to more effectively investigate and remedy Privacy Act and other violations. The Discoverability of Information approach should employ an automated process of requesting and documenting information sharing to enhance the audit capability of the system. The XML Segregation of Information approach provides the highest level of compliance with the Privacy Act, since it significantly reduces the individual FBI user role in the decision to share information, while maintaining the most robust audit trail of the information sought, reviewed and shared by each individual user and agency. All of these approaches require or may require some manual sharing, which creates at least some potential for Privacy Act violations in the actual sharing of the terrorism and homeland security information

consistent with the "status quo" approach with its dependence on the judgment and execution by the individual FBI employee or TFO.

The above analysis resulted in the following ratings for these four approaches (Table 9).

Table 9. Privacy Act Compliance Criteria Ratings

Criteria	Status Quo	HLS Routine Use	Discoverability of Information	XML Segregation of Information
Privacy Act Compliance	Medium	Medium	Medium	High

c. Privacy Impact Assessment

The following PIA Section 5 was created for the current FBI "status quo" approaches to information sharing:

> **Section 5.0 External Sharing and Disclosure**
>
> The following questions are intended to define the content, scope, and authority for information sharing external to DOJ, which includes foreign, federal, state and local government, and the private sector.
>
> **5.1 With which external (non-DOJ) recipient(s) is the information shared?**
>
> The information is shared with all federal, state, local and tribal agencies with a "need to know" the information that meets a current FBI blanket "routine use" exceptions or other lawful basis to receive the information.
>
> **5.2 What information is shared and for what purpose?**
>
> The current "status quo" shares information that establishes a violation of law, regulation, rule, order or contract. The information may be disclosed to the entity responsible for its enforcement, including federal, state, local and tribal agencies.

5.3 How is the information transmitted or disclosed?

The information can be transmitted or disclosed in person, through a secure computer network, in a document or through any other reliable existing or future authorized communication means.

5.4 Are there any agreements concerning the security and privacy of the data once it is shared?

There are not any agreements concerning the security or the privacy of the data, except for the rules for whatever system or method is used to share the information. This information is still restricted by the Privacy Act after it is shared with the recipient agency. The Memorandum of Agreement (MOA) executed by the FBI and all participant agencies governs the information shared through the Joint Terrorism Task Force (JTTF) to Task Force Officers (TFOs). This MOA makes all the TFOs subject to the laws, regulations, guidelines and policies applicable to the FBI.

5.5 What type of training is required for users from agencies outside DOJ prior to receiving access to the information?

There would not be any specific training for users outside DOJ that would get access to the terrorism and homeland security information, except the training for the mechanism utilized for the actual sharing of the information. The JTTF TFOs are trained by the FBI as part of their role on the JTTF.

5.6 Are there any provisions in place for auditing the recipients' use of the information?

There are no inherent auditing mechanisms for use of the information. Existing system and policy auditing systems in the mechanism or policy actually utilized for sharing information will vary according to the system. The JTTF TFOs are supervised by a FBI Supervisor and other management and subject to existing systems to audit information sharing.

> **5.7 Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated.**
>
> The greatest privacy risks are the risks inherent with all homeland security information sharing, including the possibility that the information will be misunderstood or misinterpreted. Since this is not a computer system, there are no mechanisms inherent in this approach to minimize the further dissemination or utilization of the shared terrorism or homeland security information. Ultimately all sharing of terrorism and homeland security information requires trust in the recipient to understand and appropriately handle and use the information.

This PIA does not adequately address any sections other than sections 5.1 and 5.2. The PIA illustrates the lack of control and auditing in the current manual "ad hoc" information sharing mechanisms addressed in greater detail in earlier sections of this thesis. The PIA for the new homeland security "routine use" exception was identical to the "status quo" PIA except for Section 5.2:

> **5.2 What information is shared and for what purpose?**
>
> This approach will share appropriate terrorism and homeland security with federal, state, local and tribal agencies with a need for this information to perform their homeland security missions.

The proposed new homeland security "routine use" exception PIA suffers from the same deficiencies as the "status quo" approaches PIA due its reliance on the existing manual "ad hoc" information sharing mechanisms. Section 5.2 only addresses the expanded permissible terrorism and homeland security information sharing in this approach.

The following PIA Section 5 was created for the Discoverability of Information approach:

> **Section 5.0 External Sharing and Disclosure**
>
> The following questions are intended to define the content, scope, and authority for information sharing external to DOJ, which includes foreign, federal, state and local government, and the private sector.

5.1 With which external (non-DOJ) recipient(s) is the information shared?

The information will be shared with all federal, state, local and tribal homeland security agencies with a need to know the information to perform their homeland security mission.

5.2 What information is shared and for what purpose?

An index of all entities associated with FBI homeland security and terrorism investigations searchable by authorized users of the system will be shared in this system.

5.3 How is the information transmitted or disclosed?

The information will be accessible through a secure network, like N-DEx, Law Enforcement Online (LEO), RISSNET or a new VPN system. The system will only confirm and provide location information for potential homeland security information related to the particular entity. The user will be required to utilize existing "ad hoc" relationships and mechanisms to actually obtain the underlying information or determine that the information is not suitable for sharing.

5.4 Are there any agreements concerning the security and privacy of the data once it is shared?

This system requires a Memorandum of Understanding (MOU), like other computer systems, and is governed by a user's agreement. These would be the standard agreements utilized for other Department of Justice and FBI systems to ensure security and privacy protection.

5.5 What type of training is required for users from agencies outside DOJ prior to receiving access to the information?

A computer based training system would be required for all users of the system to obtain and maintain their access to the system.

5.6 Are there any provisions in place for auditing the recipients' use of the information?

There will be robust auditing of the access with logs and enforcement of violations of system rules. However, sharing terrorism and homeland security information will be conducted pursuant to the existing or future "ad hoc" systems and policies, and will be governed by auditing systems and rules of that system or policy.

5.7 Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated.

The most significant privacy risks are misuse of the system or information from the system. FBI auditing of usage should mitigate unauthorized or inappropriate uses of the system; however, it will be subject to the same limitations as any other government computer systems. There is a greater risk of misuse created by the greater number of users, including users not employed or directly managed by the federal government, Department of Justice or the FBI.

An authorized user will be able to conduct searches of FBI terrorism and homeland security information to determine if an individual, location or other entity is in the system. The individual will be directed to contact the appropriate entity within the FBI to determine the nature of this "positive hit." It will be possible to distinguish subjects of pending cases to indicate a possible nexus to terrorism. However, it will be clear that all other "positive hits" may not have any nexus to terrorism. The system will emphasize not taking any action based on the search results or lack of positive search results. The system will not allow for the surfing of information by the user, which will mitigate the potential privacy impact.

Once the information is provided to the authorized user(s), after being identified through the system, then the handling of it will be governed by current or future "ad hoc" systems and policies. The existing "ad hoc" systems and policies do not have robust systems for ensuring proper usage of the information, but this deficiency does not represent a problem or limitation of this proposed system.

The XML Segregation of Information PIA was identical to the Discoverability of Information PIA, except for Sections 5.2, 5.3 and portions of 5.7:

5.2 What information is shared and for what purpose?

This system will identify and segregate all different types of FBI terrorism and homeland security information contained in the FBI case management system. The type of information shared is limited according to the sensitivity of the information, the legal authority for the recipient to get the information, security clearance level of the system, security clearance of recipient and the need for the recipient to have the information to perform their homeland security mission. The information that does not meet this standard is not available to the user or in the system.

5.3 How is the information transmitted or disclosed?

The information is transmitted through a variety of secure networks or electronic media, including classified and controlled unclassified information systems. The information will be accessible through a secure network, like N-DEx, Law Enforcement Online (LEO), RISSNET or a new VPN system. The information will also be accessible through classified systems like Department of Defense's (DoD) Secret Internet Protocol Router Network (SIPRNET) and Joint Worldwide Intelligence Communications System (JWICS) connected to FBI classified networks.

5.7 Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated.

The most significant privacy risks are misuse of the system or information from the system. FBI auditing of usage should mitigate unauthorized or inappropriate uses of the system; however, it will be subject to the same limitations as any other government computer systems. There is a greater risk of misuse created by the greater number of users, including users not employed or directly managed by the federal government, Department of Justice or the FBI.

The information provided through the system will be provided to the recipient homeland security user and agency for limited

> purposes. The user will not be authorized to take action based on the information or further disseminate the information without the written permission of the FBI. There will be robust auditing and enforcement measures to address violations of these restrictions similar to the enforcement mechanisms created and being implemented for the criminal information sharing system N-DEx.

Both PIAs provide detailed information for every section of the PIA. They sufficiently address all sub-sections and provide a thorough understanding of the critical aspects of these approaches, including robust means to protect the information and audit access to the information.

Analysis of these PIAs resulted in the following ratings for the four approaches (Table 10).

Table 10. Privacy Impact Assessment Criteria Ratings

Criteria	Status Quo	HLS Routine Use	Discoverability of Information	XML Segregation of Information
Privacy Impact Assessment	Low	Low	High	High

3. Security

a. Handling of Sensitive and Classified Information

The current "status quo" and the new homeland security "routine use" exception approaches are both manual approaches completely dependent on individual users of FBI systems. The FBI ensures the appropriate vetting of all users of FBI systems, including user understanding and compliance with security restrictions designed to protect sensitive and classified information. The FBI case management systems, ACS and Sentinel, protect all information to the highest classification level, which is the Secret level for both of these FBI systems. These approaches ensure compliance with all USIC

security requirements for handling and storing classified information. This high level of security is detrimental to information portability and sharing.

The Discoverability of Information approach is a technological solution that will not contain the actual classified or sensitive information in an immediately usable manner. If the name of the entity itself is classified, then it would be restricted within the system as a "silent hit" or never entered into the system to ensure the security of the classified information. Potentially relevant information identified through this system will have a reference number, which can be utilized with existing "ad hoc" manual information sharing approaches to complete the sharing process. If the underlying information is classified or sensitive, then the FBI must comply with the necessary USIC and FBI requirements to share or withhold the information. This approach has the same limitations and vulnerabilities discussed for the "status quo" approach.

The XML Segregation of Information approach removes or anonymizes classified and sensitive information before providing it to an authorized agency or system. This enables the FBI to remove classified information from documents that are shared in systems like N-DEx that are not authorized for classified information, while retaining the classified information for classified networks like SIPRNET or HSDN. This capability could also protect other sensitive information; like grand jury information, tax information, FISA material, information from foreign governments, information from other agencies, information obtained pursuant to other federal statutes and other sensitive information. This approach ensures FBI compliance with all restrictions on all types of classified and sensitive information, while maximizing information sharing. The FBI could also protect entire document(s) or portions of documents for a limited time period or from particular recipient(s). This segregation of the different types of information gives the FBI the greatest flexibility to secure and share all types of information to the appropriate users or groups of users without revealing unnecessary or inappropriate classified or sensitive information. The classified information removed or anonymized from documents shared in an unclassified system could still be shared through the existing manual "ad hoc" processes or through classified systems like SIPRNET or

HSDN, since the classified information can only be stored, transmitted or retrieved from an authorized classified network in an authorized facility. The manual sharing process for classified and historical FBI terrorism and homeland security information creates the same potential risks of inappropriate disclosures of classified or sensitive information as the other three approaches. This XML approach facilitates attainment of the *FBI NISS* guiding principle to "[p]roduce documents at the lowest classification level feasible without losing meaning or essential context while protecting sources and vital national security information" (FBI, 2008, ¶ 6).

Analysis of the handling of classified and sensitive information in all four approaches resulted in the following ratings (Table 11).

Table 11. Sensitive/Classified Information Criteria Ratings

Criteria	Status Quo	HLS Routine Use	Discoverability of Information	XML Segregation of Information
Sensitive/Classified Info	Medium	Medium	Medium	High

b. Access Control

The "status quo" and the new homeland security "routine use" exception approaches are both manual "ad hoc" processes that do not have technological access control systems. The FBI case management systems store the majority of the terrorism and homeland security information, and both have robust access control systems. The Secret classification level for these systems prevents them from being physically connected to unclassified networks like the Internet or unclassified government networks, which significantly reduces the threat of unauthorized access by an outsider. All information systems are susceptible to the insider threat, which can ultimately result in an authorized user conducting unauthorized dissemination of the information. These systems do not handle the mechanism for information sharing, but their access control systems limit access to the information to a large group of authorized FBI system users. Therefore, the information is secure with the system users responsible for sharing

information exercising individual control over access to the information. These two approaches are dependant on authorized FBI users to determine the "who, what, where and when" of all information sharing. This distributed control creates greater vulnerability for mistakes and inconsistent application of the rules, which can create a corresponding increased risk of unauthorized access or inappropriate denial of access to information.

The Discoverability of Information and XML Segregation of Information approaches both provide significant access control through automated systems. These systems employ the same technology utilized by numerous other government and private computer systems. No system can prevent all unauthorized access or ensure everyone with authorized access is always able to access the system and all appropriate information. These two approaches enable the greatest possible access control offered by current and future security technologies. There is risk of unauthorized access to specific information in the Discoverability of Information due to its reliance on current "ad hoc" mechanisms to communicate or withhold requested information identified in this system. However, this approach creates a more robust and reliable record of access, which will be addressed in greater detail in the following section on compliance and audit capabilities. XML Segregation of Information provides the greatest level of access control permitted by the available technology deployed in the system, but the storage of any FBI information in a system outside the FBI Secret network creates a greater vulnerability in access control and other security issues.

Analysis of the access control resulted in the following ratings of these four approaches (Table 12).

Table 12. Access Control Criteria Ratings

Criteria	Status Quo	HLS Routine Use	Discoverability of Information	XML Segregation of Information
Access Control	Medium	Medium	High	High

c. Compliance and Audits

The "status quo" and new homeland security "routine use" exception approaches are manual methods primarily relying on manual auditing processes to ensure compliance. The first level of review and potential auditing in FBI information management and sharing is the FBI first line supervisor, who has the authority to approve a document and authorize information sharing to ensure it is in compliance with all FBI policies and procedures. Records of information sharing are maintained in FBI case management systems for review by FBI and DOJ-OIG personnel in future audits. These audits are completely dependant on the quality of the information reported in FBI case management systems. Manual systems also provide a greater opportunity for individuals to circumvent the authorized information sharing processes with informal information sharing that is not properly documented. Manual audits are manpower intensive and do not take place contemporaneously with the actual sharing of the information. Finally, there is a risk of misuse of information due to inadequate training. This manual process is entirely dependant on the performance of the FBI employees, who receive, share, supervise and audit the information sharing.

The Discoverability of Information and XML Segregation of Information leverage current technological approaches to review the sharing and withholding of information in a timey manner with robust auditing to ensure maximum compliance by the recipient and the FBI. Access to information logs can be stored in immutable logs, which are a secure method to protect logs from easy tampering by authorized or unauthorized users. The electronic storage of information about the actual information shared and recipient allows for compliance reviews to be conducted in a timelier manner to prevent delays in information sharing, while maintaining robust records allowing for effective comprehensive audits. These logs permit more frequent, remote audits of sharing or withholding information.

This audit capability would allow FBI management to more effectively review both the sharing and withholding of terrorism and homeland security information. Aggressive and timely compliance auditing could remedy failures to share information by

overruling the original decision to withhold information and immediately sharing the information. The timely discovery of information sharing deficiencies allows FBI management to immediately provide remedial training or take other actions to ensure improved compliance with all FBI information sharing rules and procedures. Immediate feedback to FBI users inappropriate failures to share information has the potential to improve the overall FBI information sharing effort. Review and auditing could also be employed to motivate FBI users and ensure improved compliance by clearly communicating the nature and scope of audits and consequences for failings or repeated failings. For example, a FBI user aware that refusals to share information or restricting information leads to an enhanced review process or increased likelihood of an audit is likely to be encouraged to increase their information sharing, which could counter current and future cultural, legal or other incentives to withhold information. This capacity could also ensure the protection of highly sensitive information by auditing the sharing of certain types of information. This auditing capacity and the end user's agreement (EULA) provide the FBI an opportunity to enforce information recipient violations of the policies and procedures. Resources dedicated to auditing and system rules in the MOU will define this capacity and provide the authority to investigate information recipient violations. The audit trail will be invaluable evidence to identify and substantiate violations through formalized internal processes or informally with the management of non-FBI users suspected of rules violations. The N-DEx system already has some capacity and authority for this type of auditing and enforcement actions with criminal intelligence from their computer system.

The analysis of the audit capacity and compliance capability of these four approaches resulted in the following ratings (Table 13).

Table 13. Compliance/Audit Criteria Ratings

Criteria	Status Quo	HLS Routine Use	Discoverability of Information	XML Segregation of Information
Compliance/Audit	Medium	Medium	High	High

B. IMPLEMENTATION FACTORS ANALYSIS

The second phase of the analysis examines the critical factors impacting the implementation of these approaches. This analysis is unnecessary for any system that fails on any of the implementation factors. Based on the assumption that "unknown" public perception will be met for all of these approaches, the thesis continues with the implementation analysis of all approaches in the following sections.

1. Cultural Barriers[8]

The FBI currently engages in extensive information sharing consistent with or integrated over the past few years into FBI culture. FBI employee resistance to sharing has been mitigated by FBI policies, training and efforts over the years since 9/11. The ability of individual FBI employees to unilaterally inhibit information sharing persists, which maintains some potential for cultural resistance in any particular instance or by an individual employee. The incorporation or mitigation of FBI cultural resistance into current FBI information sharing means the "status quo" approach does not face significant additional cultural resistance. It is impossible to precisely quantify the level of FBI cultural resistance, but expanded information sharing since 9/11 by FBI personnel illustrates at least some significant reduction in cultural resistance after 9/11. The expansion of permissible information sharing with the new homeland security "routine use" exception is also likely to be easily integrated into existing FBI culture to the same extent and manner as the "status quo" approach. The new homeland security "routine use" exception approach uses terms and standards familiar to FBI employees from the new *AGG-DOM* that govern all FBI investigations. These rules have governed FBI investigations and operations since October of 2008, which substantially reduces the likelihood of confusion and cultural resistance caused by introducing a new approach with unfamiliar rules and terms. However, expansion of the amount of information shared could create additional cultural resistance, since change can cause concerns that

[8] The author of this thesis relied upon personal experience in the FBI Boston Field Office for the past 12 years to assess and examine FBI culture and the impact of FBI culture on these proposed changes.

may manifest themselves as cultural resistance. The new homeland security "routine use" exception approach does not employ any technology to mitigate possible FBI cultural resistance. This new homeland security "routine use" exception is consistent with the FBI *NISS* and DNI mandate to create a culture of a "duty to provide." Unfortunately, there is no objective, reliable reporting to indicate whether this "duty to provide" has already been successfully integrated into the USIC or FBI cultures.

The Discoverability of Information and XML Segregation of Information both have significant potential for FBI cultural resistance. The FBI has experienced numerous technological changes over the years with computer systems like VCF, Sentinel, Delta, IDW and others.[9] The FBI has also gone through extensive changes involving the re-alignment of resources within the FBI, new Attorney General Guidelines, a new *Domestic Investigative Operations Guidelines (DIOG)*, the Strategic Execution Team (SET) process, creation of a Directorate of Intelligence, creation of the Weapons of Mass Destruction (WMD) Directorate, and countless other significant, substantive changes precipitated by the terrorist attacks of 9/11 and the U.S. government transformation in response to these attacks. The years of constant, substantial change have created an environment with significant potential for cultural resistance resulting from the implementation of a considerable volume of new technologies and policies. Therefore, it is probable that there will be some cultural resistance to any additional technology and policy changes.

Despite this significant potential for cultural resistance, both of these technological systems use technology to automate the process, which should significantly reduce the immediate burden and limit the potential negative impact on FBI employees. The Discoverability of Information approach could face resistance from FBI employees called upon to respond to increased requests for highly sensitive, investigative information from individuals outside the FBI from FBI employees or TFOs with responsibility for the investigation or collection of the information. The XML Segregation of Information approach should not face this obstacle as frequently as the

[9] VCF, Sentinel and IDW were examined in greater detail in earlier sections of this thesis. Delta is the new Confidential Human Source (CHS) computer system recently developed and deployed by FBI.

Discoverability of Information approach, since a significant amount of the information will be directly available from the system without direct FBI employee involvement. This reduced involvement of individual FBI employee with an interest in the case and information should reduce cultural resistance from FBI employees. There is still potential for individual FBI employees to express their resistance through the over-classification, inappropriate labeling of sensitive information or other behavior intended to inhibit information sharing through an informal method, which could reduce the amount of information shared beyond the FBI. However, this can be addressed through effective policies, supervision, robust auditing and appropriate enforcement of the rules designed to ensure the implementation of the DNI "duty to share" standard. The FBI has been navigating all of these technological changes in the middle of sweeping organizational changes, which has created concerns of "change fatigue" in the FBI.

It is extremely difficult to assess and rate the likely cultural barriers and resistance to these approaches in the FBI. Despite the inherent difficulties of conducting this analysis, the following ratings were made based on the best possible assessment of the FBI cultural barriers and technological solutions that might mitigate these issues (Table 14).

Table 14. Cultural Barriers Implementation Factor Ratings

Factor	Status Quo	HLS Routine Use	Discoverability of Information	XML Segregation of Information
Cultural Barriers	Medium	Medium	Medium	Medium

2. Fiscal Performance

The "status quo" and new homeland security "routine use" exception approaches are both manual systems that do not require substantial additional financial expenditures. The costs associated with the technologies and methods used in the "status quo" approach have already been expended or will be expended for purposes other than these approaches in the future. The new homeland security "routine use" exception would only

have minimal additional expenses beyond those in the "status quo" approach. There would be nominal expenses associated with finalizing the homeland security "routine use" exception, like getting DOJ approval, publishing it in the Federal Register, reviewing public comments, submitting it to OMB, training FBI personnel on the new rules and other miscellaneous expenses. The greatest expense for these two approaches is the continuing cost of devoting significant personnel resources to the manual process of searching and sharing information, rather than an automated, technological approach that would ameliorate some of these costs in the future.

The Discoverability of Information and XML Segregation of Information approaches both require significant financial expenditures for a new computer system or utilization of an existing system capable of performing all necessary functions, like N-DEx. The Discoverability of Information only requires a computer system as complex as Guardian. The limited requirements for these approaches should prevent the costs of the system from rising anywhere near the level of a case management system like Sentinel. The Discoverability of Information approach would only provide minimal savings of personnel expenses associated with the current "status quo" information sharing approach, since the actual sharing of information is not automated.

An essential expense for the XML Segregation of Information approach is the creation of numerous new XML forms capable of segregating the different types of classified and sensitive information collected and maintained by the FBI. The NER technology, discussed in Chapter V, does not allow for the reliable automatic creation of XML documents with all the classified and sensitive information segregated from the existing data or new free-form documents. Sentinel XML documents created by the FBI have already cost $810,000, but are currently undergoing modifications to meet FBI operational requirements (DOJ-OIG, 2009, p. 17). Additional modifications and improvements of these forms will be required to enable enhanced information sharing and address future creations of new categories of sensitive information.[10] The XML

[10] The FBI restricted most of the detailed information regarding the new XML forms for Sentinel in the most recent DOJ-OIG report on Sentinel and has not officially released the forms within the FBI, which prevents the writer from definitively determining the information sharing capabilities of those forms (DOJ-OIG, 2009).

Segregation of Information approach is substantially more complex than the other approaches, which would require a more sophisticated computer system to accomplish its objectives. This approach would provide an automated system for sharing the appropriate information actually available in the system, which would provide substantial future savings in personnel resources that are currently being utilized for the "ad hoc" manual information sharing methods. Both technology approaches may have additional expenses associated with preparing the information for different systems or data sets for the different levels of classification or sensitivity. For example, the FBI may need to create a different system to run on SIPRNET or HSDN to share classified information automatically, rather than manually. These expenses would be less substantial than creating a whole new system, since the FBI could deploy the previously developed system on a new network. The deployment of an existing system to a new network would only have the additional equipment and maintenance costs. It is also possible to significantly mitigate the vast majority of new expenditures for developing, deploying and operating a new computer system by utilizing the existing N-DEx system with minimal modifications to accommodate the additional requirements and functions necessary for the Discoverability of Information or XML Segregation of Information approaches.

All four approaches could be highly rated for the fiscal performance criteria with the utilization of an existing system like N-DEx; however, a conservative rating approach was utilized to differentiate the rating of these four approaches. Table 15 reflects the ratings for these four approaches.

Table 15. Fiscal Performance Implementation Factor Ratings

Factor	Status Quo	HLS Routine Use	Discoverability of Information	XML Segregation of Information
Fiscal Performance	High	High	Medium	Medium

3. Utilization of Technology

The "status quo" and new homeland security "routine use" exception approaches have very limited utilization of technology. The technology utilized in the existing and developing approaches was extensively detailed in Chapter IV, including computer systems like eGuardian, LEO, RISSNET and others that store unclassified information. However, none of these systems is currently being utilized to identify or communicate FBI terrorism and homeland security case related information to SLTs. They do have some limited capacity to serve this function in the future.[11] N-DEx and OneDOJ are systems currently under development, accessible through LEO, designed to share criminal intelligence that may also have incidental value as terrorism or homeland security information.

The Discoverability of Information approach requires technology to allow SLTs to quickly and effectively conduct searches of an index of entities in available FBI documents in this "pointer system." The FBI could employ NER technology to create an index of existing FBI terrorism and homeland security information from the existing free-form FBI case reporting documents. However, this approach still relies on the same current manual or automated processes of sharing terrorism and homeland security information employed by the "status quo" and new homeland security "routine use" exception approaches. Technology is a critical component of this Discoverability of Information approach, but there are vital aspects of this approach that still require FBI employees and TFOs to perform essential manual processes.

The XML Segregation of Information approach requires the most extensive utilization of technology. This approach uses XML technology to segregate the many different types of classified and sensitive information collected and maintained by the FBI. The FBI already employs XML technology for several existing forms and the new forms being developed for Sentinel. This approach will utilize technology to remove or anonymize different types of classified and sensitive information to comply with

[11] eGuardian stores SAR information, which is also stored in the FBI case management systems and may be related to an existing or future case.

restrictions of the particular system or recipient. This approach is dependent on advanced technologies to facilitate the searching and actual sharing of terrorism and homeland security information. The XML Segregation of Information approach requires a sophisticated computer-network, like N-DEx, or multiple sophisticated computer systems to address the different classification levels of the information maintained in FBI case management systems, which would require at least a Secret and a Controlled Unclassified Information system.

All four approaches are enhanced by technology; however, the difference in the role(s) of technology in these approaches resulted in the following ratings for the approaches (Table 16).

Table 16. Utilization of Technology Implementation Factor Ratings

Factor	Status Quo	HLS Routine Use	Discoverability of Information	XML Segregation of Information
Utilization of Technology	Low	Low	Medium	High

4. Training Requirements

The "status quo" approach has already been implemented with the required and supplemental training. Additional training would improve FBI performance and compliance in the "status quo" approach, which is an ongoing requirement for all information sharing approaches. The case of Major Hassan illustrates the need for improved training of FBI SAs, IAs and TFOs to enhance identification of information for sharing and compliance with the corresponding FBI policy and procedural requirements. The new homeland security "routine use" exception approach will require additional training for FBI personnel involved in this process to ensure their understanding of the enhanced scope of information that may be shared under the new policies and procedures. The FBI can leverage existing annual legal training sessions around the FBI, special training sessions and distance learning technologies, like FBI Virtual Academy, to

accomplish this training. The FBI regularly conducts training to ensure effective operations and compliance with FBI policy. The FBI is capable of providing the necessary training for these approaches without any significant, additional burden or any new approaches.

The Discoverability of Information and XML Segregation of Information approaches require much greater training. These technological approaches will be able to use the same technologies already used by the FBI to train the FBI personnel; however, these technological approaches will also have to provide some level of training to the outside agency users of the system(s). This type of training could be facilitated through the actual computer system deployed or mandated as a condition of gaining access to the system. The requirement to train individuals all around the United States with the 18,000 different law enforcement agencies and additional homeland security agencies will be an ongoing obligation for the FBI, which will require significant additional training resources on a continuing basis. The Discoverability of Information approach is dependant on a search tool that would be familiar to regular users of computers, which minimizes some of the training requirements. The training of system users is critical to ensure effective identification of the maximum amount of potentially relevant material, while limiting the amount of irrelevant material that could otherwise be erroneously identified as relevant. Inadequate training could cause system users to fail to identify critical, relevant information and may create an enormous burden on the FBI, which would be forced to dedicate additional resources for the manual review and sharing processes.

The XML Segregation of Information approach uses a more complicated system with a greater amount of information available. Therefore, the users of this system are likely to need even greater training than users of the simpler Discoverability of Information system. The XML Segregation of Information approach will also require the training of FBI personnel in the new XML forms designed and deployed with Sentinel for enhanced information sharing. This training could be conducted through existing FBI training capabilities to ensure that the over 30,000 FBI employees and all the TFOs appropriately employ the new forms to maximize information sharing capabilities. The

greatest vulnerability in this system is its dependence on the creator of the document to appropriately identify all classified and sensitive information. The FBI collectors of information could withhold unclassified, non-sensitive information by inappropriately or erroneously identifying information as classified or sensitive to prevent its efficient disclosure outside the FBI through this system. The most reliable method to minimize the potential negative consequences of both of these problems is enhanced training, which can be ensured through robust review and auditing by FBI management.

The analysis of the training requirements and capabilities resulted in the following ratings for the four approaches (Table 17).

Table 17. Training Implementation Factor Ratings

Factor	Status Quo	HLS Routine Use	Discoverability of Information	XML Segregation of Information
Training Requirements	High	Medium	Medium	Low

C. FINAL OVERALL NUMERICAL ANALYSIS

In order to facilitate overall analysis of these approaches and compare their relative value, the ratings have been aggregated and converted into the numerical values described in Chapter III. These tables provide the both effectiveness factors and criteria with numerical values and totals for all approaches. Table 18 represents the ratings developed in the analysis in this chapter with a higher overall score representing a more effective information sharing approach.

Table 18. Overall Effectiveness Factors and Criteria for the Four Approaches

Effectiveness Factors and Criteria	Status Quo		HLS "Routine Use" Exception		Discoverability of Information		XML Segregation of Information	
	Rating	Pts	Rating	Pts	Rating	Pts	Rating	Pts
Information Shared								
Relevance	Medium	2	High	3	Medium	2	Medium	2
Accuracy	Medium	2	High	3	Medium	2	High	3
Timeliness	Low	1	Low	1	Medium	2	High	3
Information Rating		5		7		6		8
Privacy Protection								
Public Perceptions	Medium	2	Unknown	*	Unknown	*	Unknown	*
Privacy Act	Medium	2	Medium	2	Medium	2	High	3
Privacy Impact Assessment	Low	1	Low	1	High	3	High	3
Privacy Rating		5		3 - 6[12]		5 - 8[12]		6 - 9[12]
Security								
Sensitive/ Classified Info	Medium	2	Medium	2	Medium	2	High	3
Access Control	Medium	2	Medium	2	High	3	High	3
Compliance/ Audit	Medium	2	Medium	2	High	3	High	3
Security Rating		6		6		8		9
Total Effectiveness Rating Score		16		16 - 19[12]		19 - 22[12]		23 - 26[12]

[12] Rating range is due to variance between no, low, medium and high ratings for public perception effectiveness rating.

Analysis of the proposed approaches' likely public perception is complicated by the inability to accurately predict public perception prior to the attempted implementation of any approach. Therefore, variance analysis was used to determine the potential impact of public perception on the privacy protection effectiveness factor. It is highly unlikely that a new or proposed system will achieve the level of performance or projected performance in protecting privacy required for a high public perception rating. This high level of public confidence system performance on privacy protection is almost certainly going to require the system to perform at a high level for some period of time with appropriate review by a trusted entity or individual(s) to confirm enhanced performance. The variance analysis will consider all three possible ratings to determine the impact of all three on the privacy protection and overall ratings. The minimum rating is low, which generates 1 point for the privacy protection evaluation factor and the overall effectiveness evaluation. The rating for the "status quo" was maintained consistent throughout the variance analysis. The potential impacts of all variations on the privacy protection results for each approach are represented in Figure 4.

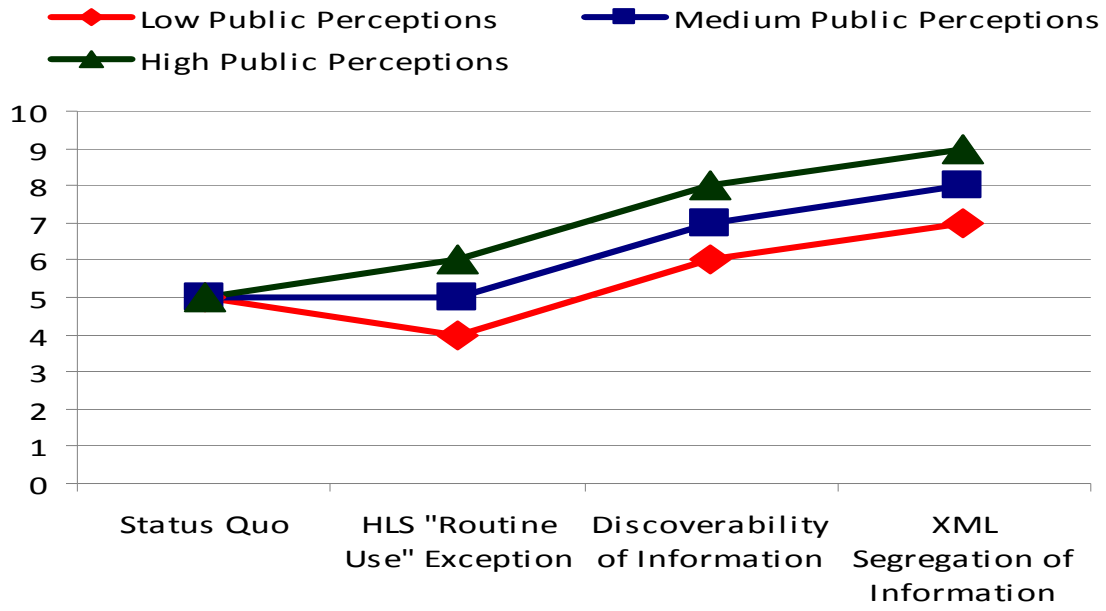


Figure 4. Variance Analysis for Privacy Protection Impact of Public Perception Criterion

This variance analysis demonstrates that the only option within an overall privacy protection rating lower than the "status quo" is the "low" rating for the homeland security "routine use" exception. All other variations resulted in an overall privacy protection rating of equal to or greater than the "status quo" approach privacy protection rating. This variance analysis was extended to the overall effectiveness factor ratings, which is reflected on Figure 5.

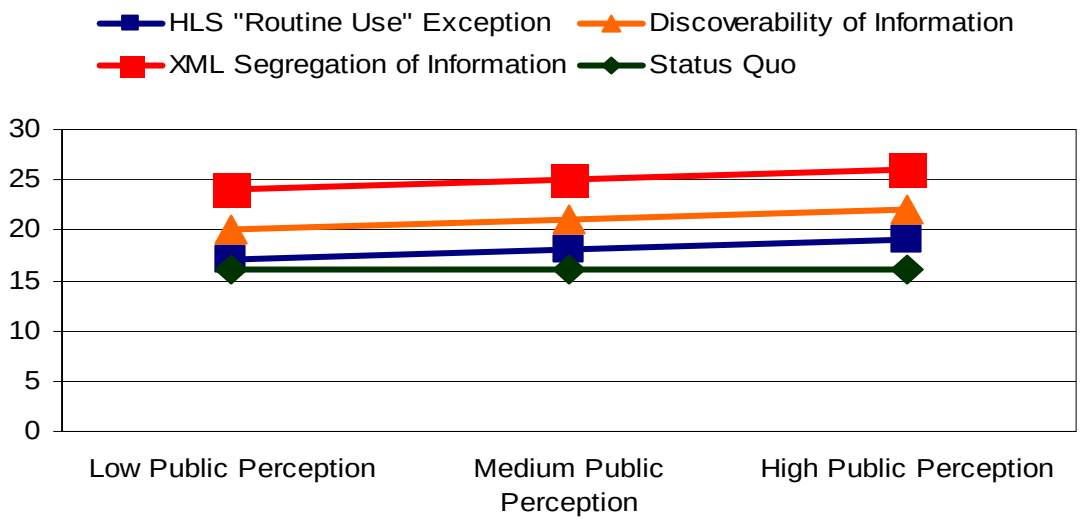


Figure 5. Variance Analysis for Impact of Public Perception Ratings on Overall Effectiveness Factor Ratings

This overall variance analysis demonstrates that the potential variations of public perception cannot result in an overall rating below the "status quo." Furthermore, the highest overall rating for each approach is still below the lowest rating for the next approach, which confirms that the variation of this single criterion will not change the overall relationship between the ratings of all four approaches.

The effectiveness and implementation rating scores for each of the approaches demonstrates they all have the potential to improve FBI terrorism and homeland security information sharing with SLT agencies. Although public perception has been a major obstacle to several high-profile homeland security related information initiatives, the variance analysis and overall evaluation demonstrate that the inability to effectively and accurately rate public perception will not significantly impact the overall analysis.

VII. CONCLUSION

> The FBI is committed to sharing timely, relevant, and actionable intelligence to the widest appropriate audience. Effective information exchange with federal agencies; state, local, and tribal officials; foreign partners; and the private sector is an increasingly important component to the FBI's unique and important national security and law enforcement mission. The FBI is required to effectively balance the need to effectively and securely share information with its responsibility to protect sources, investigative operations, national security information, and the privacy and civil liberties of US persons. (FBI, 2008, ¶ 2)
>
> —FBI National Information Sharing Strategy Vision Statement

Since 9/11, the FBI has substantially improved information sharing. However, this thesis demonstrates the potential for continued improvement of terrorism and homeland security information sharing with SLT homeland security agencies.

A. OVERALL EFFECTIVENESS OF APPROACHES

The two-phase analysis determined that all of the proposed approaches improve FBI information sharing over the "status quo." Although the implementation factor ratings varied for each of the approaches, the overall rating of implementation for all of the proposed approaches was the same. Therefore, the primary focus should be on the effectiveness factors and criteria that represent the potential performance of each of these approaches. Figure 6 illustrates the overall effectiveness performance for each of these proposed approaches derived from the analysis and ratings in this thesis.

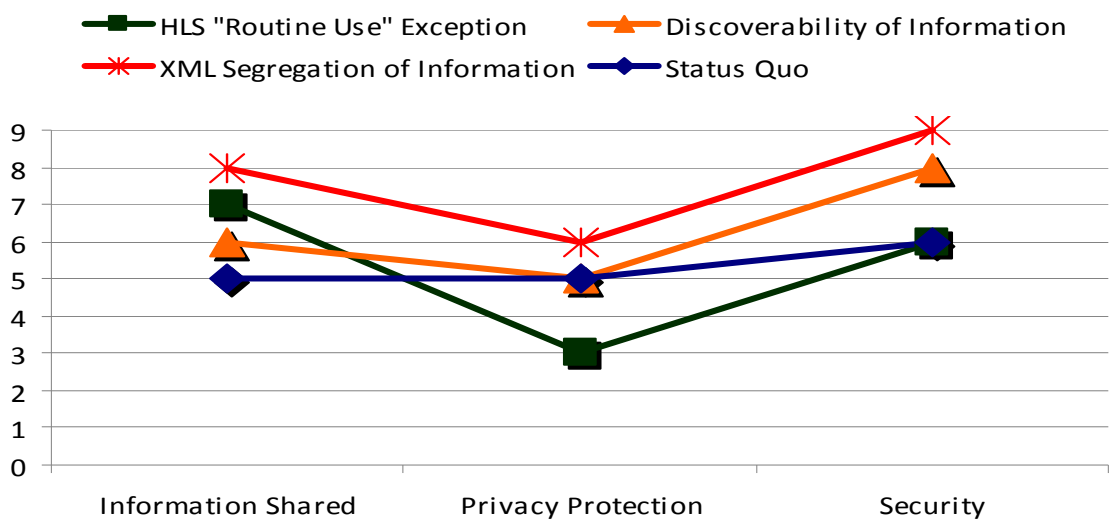


Figure 6. Overall Effectiveness of Approaches

The XML Segregation of Information outperformed all the other approaches by a significant measure due to its technological superiority to the other approaches. In fact, the level of performance for XML Segregation of Information approach overcomes the complications created by the inability to predict public perception in this methodology, since it exceeds the 2-point margin of error created by this complication. Despite the clear advantages of the two technological approaches, the FBI should still address the following questions to select the best approach for the FBI:

1. How much information does the FBI want to share with SLT agencies?
2. How effectively does the FBI want to share this information?

1. How Much to Share?

The FBI currently shares U.S. Person information covered by the Privacy Act when it relates to a violation of law, regulation, rule, order or contract. The FBI can continue this level of information sharing with its possible confusion and inconsistency caused by individual employee interpretations of these restrictions, by taking no action to expand the current "routine use" exceptions. This thesis created and analyzed a new homeland security "routine use" exception to expand the scope of this sharing to all

relevant terrorism and homeland security information related to an investigation with some level of predication (i.e., suspicion or allegation of a terrorism threat). FBI Executive Management will first need to determine whether to continue utilizing the "status quo" or expanding the information shared with the new homeland security "routine use" exception. This decision will be highly influenced by the public perception effectiveness criteria, which is impossible to accurately predict. The FBI needs to decide if the public perception and any corresponding Congressional and Executive Branch response will prevent the successful implementation of an approach using the new homeland security "routine use" exception. This new homeland security "routine use" exception was the only approach to receive a high rating for "relevant information shared" with SLT homeland security agencies. The performance of the technological approaches on the two other criteria for information shared overcame this benefit in the overall analysis; however, it is a crucial criterion to re-consider in the final selection of approaches. Figure 7 reflects the performance of all four approaches on the information shared criteria to demonstrate the impact of this on the overall ratings:

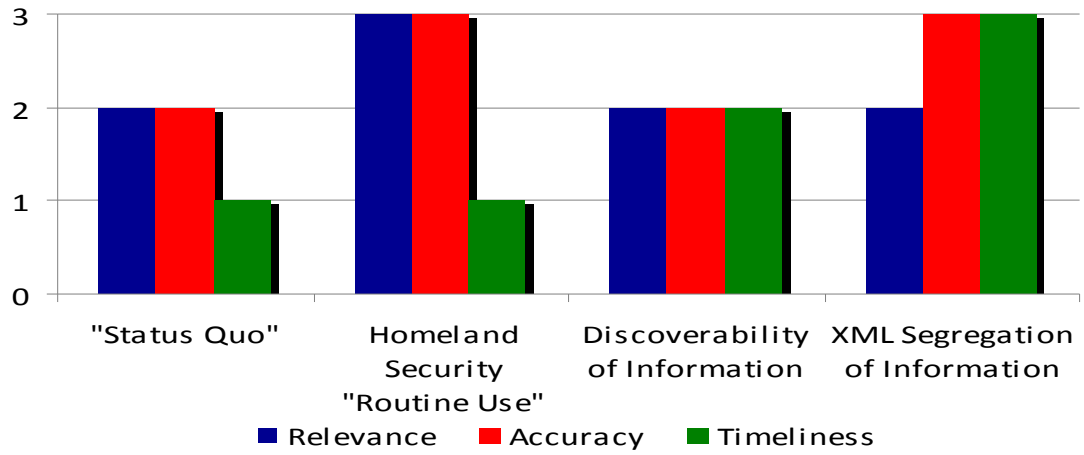


Figure 7. Information Shared Performance for All Approaches

2. How to Share?

Once the FBI determines the scope of the information to share, the next question will reveal the best approach for sharing this information with SLT homeland security

agencies. Phase one analysis of the two technological approaches clearly demonstrates the potential for the Discoverability of Information and XML Segregation of Information approaches to enhance the information shared, privacy protected and security over the current "status quo" manual methods of sharing regardless of the scope of the information shared in these systems. These two approaches complement one another, since it is not feasible to effectively integrate the historical and classified information into the XML Segregation of Information approach. The FBI needs to determine the extent of technology for expanded information sharing with SLT homeland security agencies. The Discoverability of Information approach offers a simpler, cheaper technological approach, which unfortunately has a corresponding limitation in performance requiring manual sharing mechanisms. The XML Segregation of Information approach is more complex and expensive with a corresponding increase in information sharing effectiveness. The FBI needs to determine the level of expense and technology it can feasibly commit to implement enhanced information sharing.

B. COMBINATION OF MULTIPLE APPROACHES

All of the proposed approaches must effectively integrate the "status quo" approach, since it represents the current FBI foundation for all FBI information management and sharing. The thesis methodology is effective for analyzing the combinations as a group, but not for comparing combinations with individual approaches. It provides an effective way to measure interactions if the scale were extended or if all approaches were evaluated on the same scale (e.g., some of the combined approach(es) would score high and the individual approaches less than high) This potential to enhance the overall information sharing efforts of the FBI requires some consideration of the integration of these approaches.

The new homeland security "routine use" exception allows greater terrorism and homeland security information sharing with SLTs. Therefore, this approach would enhance the quantity and quality of terrorism and homeland security information shared through the two technological approaches. Similarly the Discoverability of Information and XML Segregation of Information approaches enhance one another by enabling more

expansive and effective FBI terrorism and homeland security information sharing. The Discoverability of Information approach would most effectively handle existing non-XML, free-form FBI reporting documents, while the XML Segregation of Information would most effectively handle new FBI terrorism and homeland security information collected and reported in new XML reporting documents.

The combination of multiple approaches could also enhance the negative aspects of each of the proposed approaches. For example, the combination of multiple approaches could create a greater public concern over perceived privacy intrusions compared with deploying each approach individually. However, the method and timing of the announcement and deployment of multiple systems could mitigate this negative impact or enhance the likelihood of successful implementation of the different approaches. Assessing public perception of an individual approach was extremely complicated, but it is even more complicated to assess the likely public perception of combination approaches.

There is potential for some mitigation of the implementation factors analyzed in phase two with combination systems. The burden of an additional approach is likely to be less than the implementation of all approaches individually. For example, the two technological approaches could be integrated into a single system, which should reduce cost, maximize utilization of technology and reduce training requirements. Similarly, the combination of the new homeland security "routine use" exception with either or both of the technological approaches would not result in a significant additional burden from the three implementation factors. The implementation factor that could be significantly complicated by combination approaches is the cultural barriers, since opposition to any of the approaches in a combination is likely to result in FBI cultural resistance to the entire system or approach.

C. RECOMMENDATION

The combination approaches could have a dramatic improvement in overall information sharing with SLT homeland security agencies. The ideal approach would utilize all three approaches to complement one another and accomplish the greatest level

of information shared, privacy protected and security. This approach ensures the broadest scope of information shared by utilizing the new homeland security "routine use" exception. The FBI would need to publish the new homeland security "routine use" exception in the Federal Register with appropriate opportunity for comment by the public and OMB. This combination approach would employ the Discoverability of Information approach to maximize the sharing of historical and classified information not suitable for the XML Segregation of Information approach. Finally, the XML Segregation of Information approach offers the greatest flexibility for sharing information, protecting privacy and ensuring security for all new information collected by the FBI using the new XML forms to segregate the different types of sensitive and classified information.

The FBI made significant progress with the creation of N-DEx for sharing criminal intelligence information between federal and SLT law enforcement agencies. This system will cost almost $250 million and could easily be utilized to share terrorism and homeland security information with federal and SLT agencies. The recommended approach would utilize NER technologies to index the historical FBI information for a Discoverability of Information approach that could be integrated into N-DEx. A comparable system should be created on DoD SIPRNET and DHS HSDN networks to enable the sharing of the classified information through an automated system with other federal entities and fusion centers with access to these classified networks.

This recommended combination approach would ensure the greatest possible sharing of terrorism and homeland security information with SLT homeland security agencies. The increased information sharing with SLT homeland security agencies could also easily be expanded to the other federal homeland security agencies by simply giving them their own access to the systems. This recommended approach provides the greatest flexibility in implementation, since the FBI will achieve an information sharing improvement through the implementation of any single or combination of these approaches. Therefore, if the FBI is unable to get the funding for a new XML Segregation of Information approach due to public perception and governmental reaction, there would still be a benefit from implementing the new homeland security "routine use" exception or the Discoverability of Information

approaches. The recommended approach also enables the FBI to expand information sharing in either a piecemeal or comprehensive implementation manner.

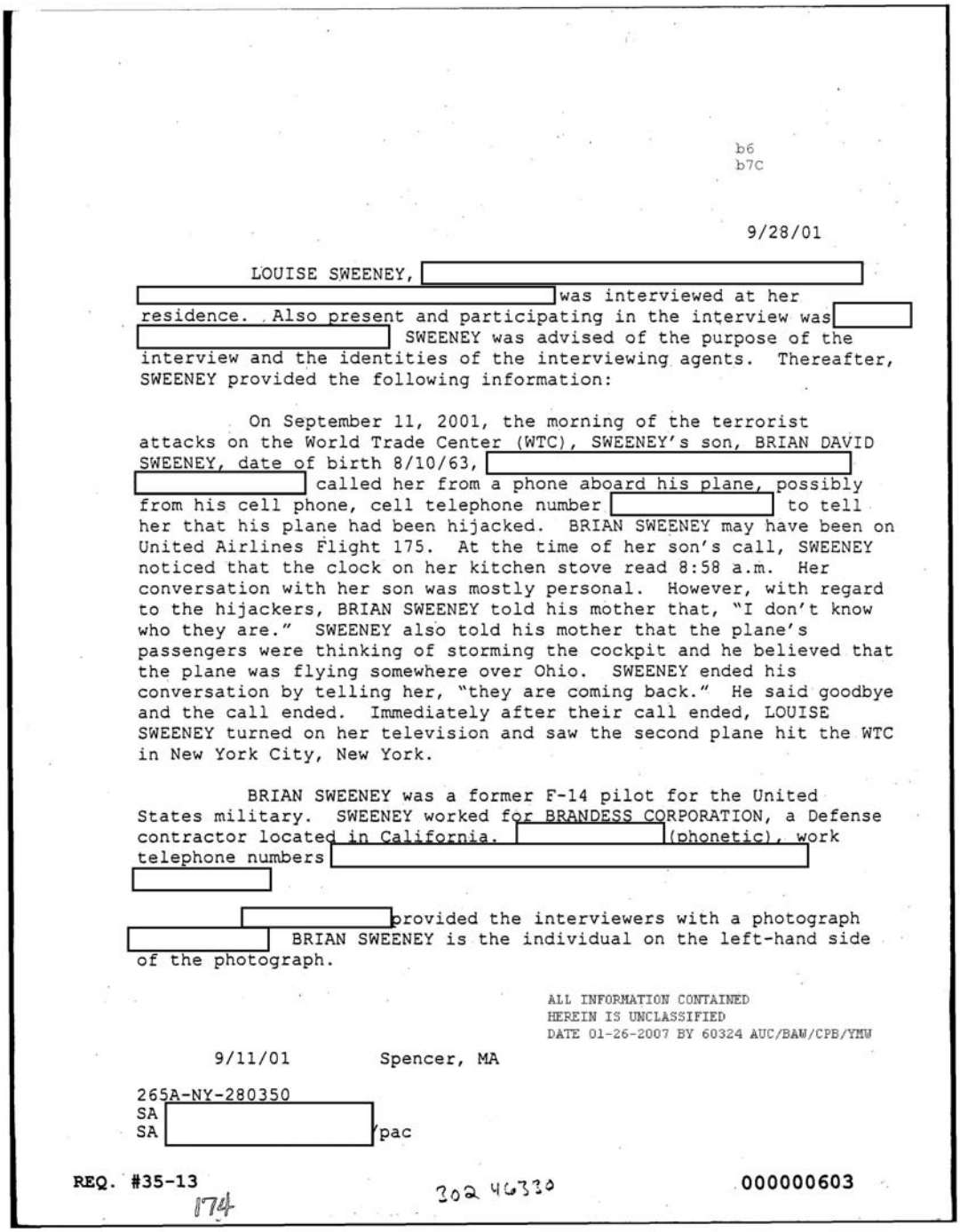
D. THE FUTURE OF FBI INFORMATION SHARING

The "status quo" clearly demonstrates a dramatic improvement in FBI information sharing in the 9 years of FBI transformation since the 9/11 attacks. The FBI could continue these "ad hoc" approaches and wait for a federal government-wide solution, while dedicating resources to other ongoing transformation projects. The FBI demonstrated its commitment to criminal information sharing with the creation and ongoing implementation of N-DEx and the pursuit of terrorism suspicious activity with the creation and implementation of eGuardian. The FBI should expand this recent history of initiative taking by creating a system to significantly expand terrorism and homeland security information sharing with SLTs. The impending deployments of Sentinel and N-DEx have paved the way for this next step of fully integrating the SLT agencies into the overall homeland security effort. Utilizing any individual or combination of the approaches proposed in this thesis would enable the FBI to more fully integrate the SLTs into the overall homeland security effort. This would also clearly demonstrate FBI commitment to joint homeland security and counterterrorism efforts with SLTs, and its trust of SLT partners with its most sensitive and critical terrorism and homeland security information.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX

Figure 8. FBI FD-302 (From FBI, n.d. (c))



b6
b7C

9/28/01

LOUISE SWEENEY, [redacted] was interviewed at her residence. Also present and participating in the interview was [redacted] SWEENEY was advised of the purpose of the interview and the identities of the interviewing agents. Thereafter, SWEENEY provided the following information:

On September 11, 2001, the morning of the terrorist attacks on the World Trade Center (WTC), SWEENEY's son, BRIAN DAVID SWEENEY, date of birth 8/10/63, [redacted] called her from a phone aboard his plane, possibly from his cell phone, cell telephone number [redacted] to tell her that his plane had been hijacked. BRIAN SWEENEY may have been on United Airlines Flight 175. At the time of her son's call, SWEENEY noticed that the clock on her kitchen stove read 8:58 a.m. Her conversation with her son was mostly personal. However, with regard to the hijackers, BRIAN SWEENEY told his mother that, "I don't know who they are." SWEENEY also told his mother that the plane's passengers were thinking of storming the cockpit and he believed that the plane was flying somewhere over Ohio. SWEENEY ended his conversation by telling her, "they are coming back." He said goodbye and the call ended. Immediately after their call ended, LOUISE SWEENEY turned on her television and saw the second plane hit the WTC in New York City, New York.

BRIAN SWEENEY was a former F-14 pilot for the United States military. SWEENEY worked for BRANDESS CORPORATION, a Defense contractor located in California. [redacted] (phonetic), work telephone numbers [redacted]

[redacted] provided the interviewers with a photograph [redacted] BRIAN SWEENEY is the individual on the left-hand side of the photograph.

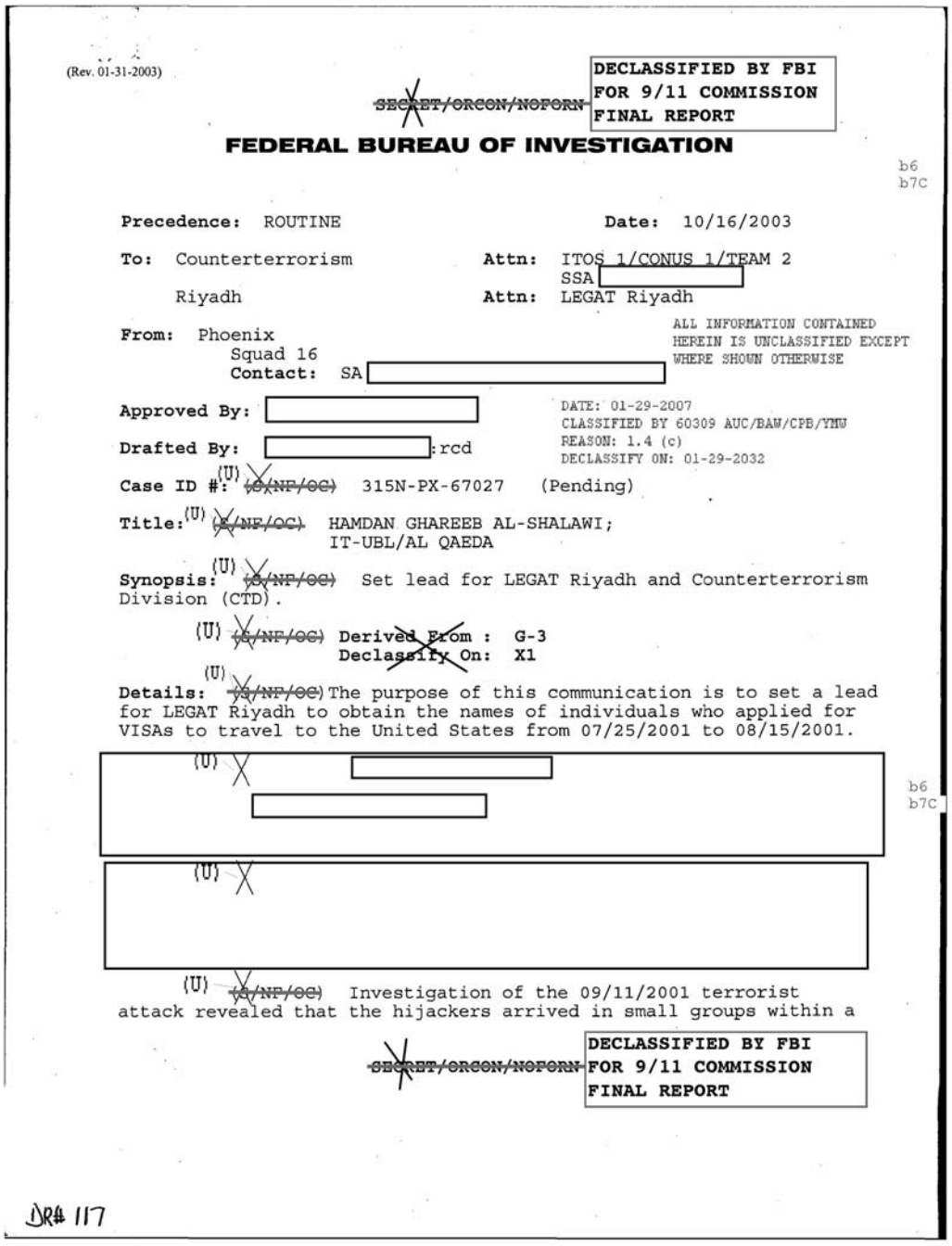
ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 01-26-2007 BY 60324 AUC/BAW/CPB/YMW

9/11/01 Spencer, MA

265A-NY-280350
SA [redacted]
SA [redacted] /pac

REQ. #35-13 174 302 46330 000000603

Figure 9. FBI Electronic Communication (EC) (From FBI, n.d. (c))[13]



(Rev. 01-31-2003)

~~SECRET/ORCON/NOFORN~~

DECLASSIFIED BY FBI
FOR 9/11 COMMISSION
FINAL REPORT

FEDERAL BUREAU OF INVESTIGATION

b6
b7C

Precedence: ROUTINE **Date:** 10/16/2003

To: Counterterrorism **Attn:** ITOS 1/CONUS 1/TEAM 2
SSA [redacted]

Riyadh **Attn:** LEGAT Riyadh

From: Phoenix
Squad 16
Contact: SA [redacted]

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Approved By: [redacted]

Drafted By: [redacted]:rcd

DATE: 01-29-2007
CLASSIFIED BY 60309 AUC/BAW/CPB/YMW
REASON: 1.4 (c)
DECLASSIFY ON: 01-29-2032

Case ID #: (U) ~~(S/NF/OC)~~ 315N-PX-67027 (Pending)

Title: (U) ~~(S/NF/OC)~~ HAMDAN GHAREEB AL-SHALAWI;
IT-UBL/AL QAEDA

Synopsis: (U) ~~(S/NF/OC)~~ Set lead for LEGAT Riyadh and Counterterrorism Division (CTD).

(U) ~~(S/NF/OC)~~ **Derived From : G-3**
Declassify On: X1

Details: (U) ~~(S/NF/OC)~~ The purpose of this communication is to set a lead for LEGAT Riyadh to obtain the names of individuals who applied for VISAs to travel to the United States from 07/25/2001 to 08/15/2001.

(U) [redacted]

b6
b7C

(U) [redacted]

(U) ~~(S/NF/OC)~~ Investigation of the 09/11/2001 terrorist attack revealed that the hijackers arrived in small groups within a

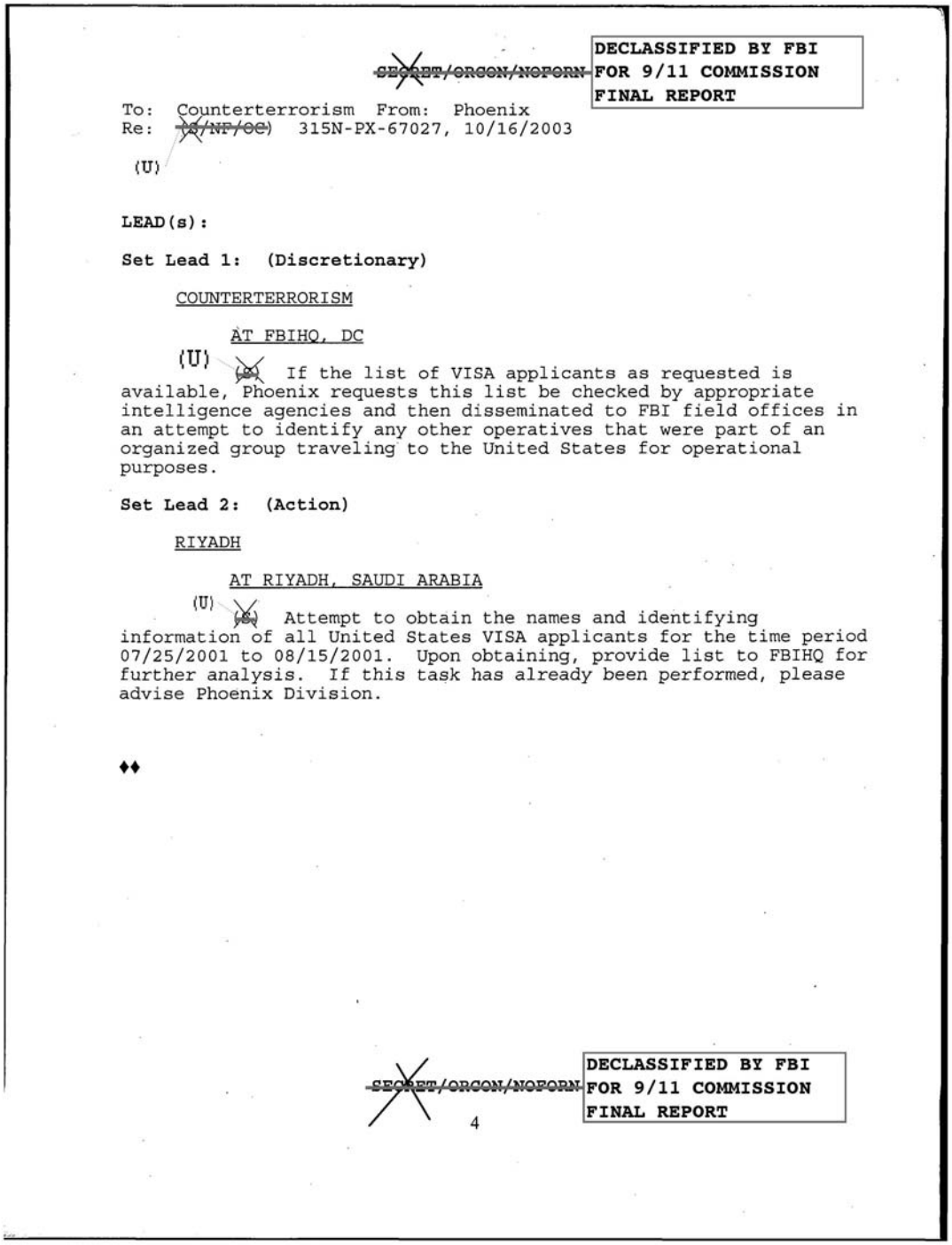
~~SECRET/ORCON/NOFORN~~

DECLASSIFIED BY FBI
FOR 9/11 COMMISSION
FINAL REPORT

DR# 117

[13] The FBI declassified this EC as a supporting document for the 9/11 Commission Final Report. It is publicly available on the FBI Internet site at the following URL: http://foia.fbi.gov/filelink.html?file=911commreport/reportdocs_110-174.pdf

Figure 10. Leads Page from EC (From FBI, n.d. (c))13



~~SECRET/ORCON,NOFORN~~

DECLASSIFIED BY FBI
FOR 9/11 COMMISSION
FINAL REPORT

To: Counterterrorism From: Phoenix
Re: ~~(S/NF/OC)~~ 315N-PX-67027, 10/16/2003

(U)

LEAD(s):

Set Lead 1: (Discretionary)

COUNTERTERRORISM

AT FBIHQ, DC

(U) ~~(S)~~ If the list of VISA applicants as requested is available, Phoenix requests this list be checked by appropriate intelligence agencies and then disseminated to FBI field offices in an attempt to identify any other operatives that were part of an organized group traveling to the United States for operational purposes.

Set Lead 2: (Action)

RIYADH

AT RIYADH, SAUDI ARABIA

(U) ~~(S)~~ Attempt to obtain the names and identifying information of all United States VISA applicants for the time period 07/25/2001 to 08/15/2001. Upon obtaining, provide list to FBIHQ for further analysis. If this task has already been performed, please advise Phoenix Division.

♦♦

~~SECRET/ORCON,NOFORN~~

DECLASSIFIED BY FBI
FOR 9/11 COMMISSION
FINAL REPORT

4

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

5 U.S.C. § 552a(a)(2).

5 U.S.C. § 552a(a)(4).

5 U.S.C. § 552a(b).

5 U.S.C. § 552a(e)(4)(D).

The Attorney General's guidelines for domestic FBI operations (AGG-DOM) (2008). . Washington, DC: U.S. Department of Justice. Retrieved April 15, 2010, from http://www.justice.gov/ag/readingroom/guidelines.pdf

Bachmann, R., & Zaheer, A. (2006). *Handbook of trust research*. Cheltenham, UK: Northampton, MA: Edward Elgar.

Bajaj, A., & Ram, S. (2007). A comprehensive framework towards information sharing between government agencies. *International Journal of Electronic Government Research, 3*(2), 29.

Bald, G. (2005). Federal Bureau of Investigation, Executive Assistant Director National Security Branch, statement before the United States Senate Committee on the Judiciary on September 21, 2005: Committee on the Judiciary, U.S. Senate. Retrieved April 15, 2010, from http://www.fbi.gov/congress/congress05/bald092105.htm

Black, K. (2009, October). Nationwide suspicious activity reporting initiative. *Community Policing Dispatch*, 2. Retrieved April 15, 2010, from http://www.cops.usdoj.gov/html/dispatch/November_2009/nsi.htm

Boyle, L. C. (2007). *Memorandum of understanding on terrorist watchlist redress procedures.* Retrieved September 1, 2009, from http://www.fbi.gov/terrorinfo/counterrorism/redress_mou.htm

Bundestag. (2006). Act on setting up joint databases of police authorities and intelligence services of the federal government and the Länder (Act on Joint Databases) of 2006, Retrieved April 15, 2010, from http://www.en.bmi.bund.de/cln_012/nn_1016300/Internet/Content/Common/Anlagen/Gesetz/Antiterrordateigesetz__en,templateId=raw,property=publicationFile.pdf/Antiterrordateigesetz_en.pdf

Cook, K. S., Hardin, R., & Levi, M. (2005). *Cooperation without trust?* New York: Russell Sage Foundation.

Dempsey, J. X., & Rosenzweig, P. (2004). Technologies that can protect privacy as information is shared to combat terrorism. *Legal Memorandum, 11*, 1–12. Retrieved April 15, 2010, from http://www.heritage.org/Research/HomelandSecurity/lm11.cfm

Department of Justice Office of Inspector General (DOJ-OIG). (2005). *The Department of Justice's terrorism task forces* (Evaluations and Inspections Report No. I-2005-007). Washington, DC: Department of Justice Office of Inspector General. Retrieved April 15, 2010, from http://www.justice.gov/oig/reports/plus/e0507/index.htm

Department of Justice Office of Inspector General (DOJ-OIG). (2007). *Audit of the department of justice information technology studies, plans, and evaluations* (No. OIG Audit Report 07-39). Washington, DC: Retrieved April 15, 2010, from http://www.justice.gov/oig/reports/plus/a0739/app6.htm

Department of Justice Office of Inspector General (DOJ-OIG). (2008). *Sentinel audit IV: Status of the Federal Bureau of investigation's case management system* (Audit Report No. 09-05). Washington, DC: Retrieved April 20, 2010, from http://www.justice.gov/oig/reports/FBI/a0905/final.pdf

Department of Justice Office of Inspector General (DOJ-OIG). (2009). *Sentinel audit V: Status of the Federal Bureau of Investigation's case management system* (Audit Report No. 10-03). Washington, DC: Retrieved 4/20/2010, from http://www.justice.gov/oig/reports/FBI/a1003_redacted.pdf

Department of Justice Office of Inspector General (DOJ-OIG). (2010). *Status of the Federal Bureau of Investigation's implementation of the Sentinel project* (No. 10-22). Washington, DC: Department of Justice Office of Inspector General. Retrieved April 20, 2010, from http://www.justice.gov/oig/reports/FBI/a1022.pdf

Electronic Frontier Foundation. (2009). *Report on the Investigative Data Warehouse.* Electronic Frontier Foundation. Retrieved April 15, 2010, from http://www.eff.org/issues/foia/investigative-data-warehouse-report

FBI Domestic Investigations and Operations Guide (DIOG). (2008). Retrieved February 20, 2010, from http://foia.fbi.gov/foiaindex/diog.htm

Federal Bureau of Investigation (FBI). (2007, January). *FBI N-DEx privacy impact assessment- January 2007.* Retrieved January 26, 2010, from http://foia.fbi.gov/piandex040607.htm

Federal Bureau of Investigation (FBI). (2008). *Federal Bureau of Investigation–National Information Sharing Strategy (NISS).* Washington, DC: FBI. Retrieved April 15, 2010, from http://www.fbi.gov/publications/niss.htm

Federal Bureau of Investigation (FBI). (2008, April 21). *FB —N-DEx - Press room - Headline archives 04-21-08.* Retrieved January 20, 2010, from http://www.fbi.gov/page2/april08/ndex_042108.html

Federal Bureau of Investigation (FBI). (2008, September 19). *FBI—eGuardian-press room-headline archives 09-19-08.* Retrieved February 14, 2010, from http://www.fbi.gov/page2/sept08/eguardian_091908.html

Federal Bureau of Investigation (FBI). (2009, November 11). *Federal Bureau of Investigation–Press release.* Retrieved November 11, 2009, from http://www.fbi.gov/pressrel/pressrel09/forthood111109.htm

Federal Bureau of Investigation (FBI). (n.d. (a)). *FBI—Law Enforcement Online (LEO).* Retrieved January 26, 2010, from http://www.fbi.gov/hq/cjisd/leo.htm

Federal Bureau of Investigation (FBI). (n.d. (b)). *FBI—Terror task forces.* Retrieved September 1, 2009, from http://www.fbi.gov/page2/may09/jttfs_052809.html

Federal Bureau of Investigation (FBI). (n.d. (c)). *911commreport/reportdocs_110-174.pdf.* Retrieved October 12, 2009, from http://foia.fbi.gov/filelink.html?file=911commreport/reportdocs_110-174.pdf

Federal Bureau of Investigation (FBI). (n.d. (d)). *FBI Privacy Act systems–70 FR 7513, 7517.* Retrieved September 1, 2009, from http://foia.fbi.gov/privacy_systems/70fr7513_brus.htm

Federal Bureau of Investigation (FBI). (n.d. (e)). *Today's FBI: Information Sharing–Facts & Figures.* Retrieved April 25, 2010, from http://www.fbi.gov/facts_and_figures/information_sharing.htm

Federal Bureau of Investigation (FBI). (n.d. (f)). *FBI Privacy Act systems–66 FR 33558, 33559.* Retrieved September 1, 2009, from http://foia.fbi.gov/privacy_systems/66fr33558_brus.htm

Federal Bureau of Investigation (FBI). (n.d. (g)). *Federal Bureau of Investigation–Directorate of Intelligence–intelligence defined.* Retrieved February 2, 2010, from http://www.fbi.gov/intelligence/di_defined.htm

Federal Bureau of Investigation (FBI). (n.d. (h)). *Federal Bureau of Investigation–Facts & figures.* Retrieved April 16, 2010, from http://www.fbi.gov/facts_and_figures/intelligence.htm

Federal Bureau of Investigation (FBI). (n.d. (i)). *Federal Bureau of Investigation - Freedom of information Privacy Act.* Retrieved February 6, 2010, from http://foia.fbi.gov/privacy_assessments.htm

Federal Bureau of Investigation (FBI). (n.d. (j)). *Federal Bureau of Investigation–N-DEx: Concept.* Retrieved February 14, 2010, from http://www.fbi.gov/hq/cjisd/ndex/ndex_concept.htm

Federal Bureau of Investigation (FBI). (n.d. (k)). *Federal Bureau of Investigation - Terrorism.* Retrieved April 16, 2010, from http://www.fbi.gov/terrorism/terrorism.htm

Federal Bureau of Investigation. (2009, June 26). *Inside the FBI's internet tip line.* Retrieved February 13, 2010, from http://www.fbi.gov/multimedia/tips062609/transcript.htm

Fine, G. (2002, March 21). *OIG testimony of Inspector Glenn Fine–March 21, 2002.* Retrieved January 24, 2010, from http://www.justice.gov/oig/testimony/0203a.htm

General Accountability Office (GAO). (2006). Information sharing: The federal government needs to establish policies and processes for sharing terrorism-related and Sensitive But Unclassified Information: GAO-06-385. *GAO Reports*.

Harold, E. R., & Means, W. S. (2004). *XML in a nutshell* (3rd ed.). Beijing; Sebastopol, CA: O'Reilly.

Healy T. (2009, December 9). Terrorist Screening Center Director, Federal Bureau of Investigation, statement before the Senate Homeland Security and Governmental Affairs Committee on December 9, 2009: Homeland Security and Governmental Affairs Committee, U.S. Senate. Retrieved April 15, 2010, from http://www.fbi.gov/congress/congress09/healy120909.htm

Hennessey, J. T., Jr. (1998). "Reinventing" government: Does leadership make the difference? *Public Administration Review, 58*(6), 522.

Hexmoor, H., Wilson, S., & Bhattaram, S. (2006). A theoretical inter-organizational trust-based security model. *The Knowledge Engineering Review, 21*(2).

Higgins, S. (2002, July 16). *Congressional testimony of Sherry Higgins, Project Management Executive for the Office of the Director, FBI before the Senate Judiciary Subcommittee on Administrative Oversight and the Courts on July 16, 2002.* Retrieved January 25, 2010, from http://www.fbi.gov/congress/congress02/higgins071602.htm

Kasper, D. V. S. (2005). The Evolution (or Devolution) of Privacy. *Sociological Forum, 20*(1), 69–92.

Liu, P., & Chetal, A. (2005). Trust-Based Secure Information Sharing Between Federal Government Agencies. *Journal of the American Society for Information Science & Technology, 56*(3), 283–298. doi:10.1002/asi.20117

MacDonald, H. (2004, Apr 1). The 'privacy' jihad. *Wall Street Journal*, p. A.14.

Markle Foundation Task Force. (2002). *Protecting America's freedom in the information age*. New York: Markle Foundation. Retrieved April 15, 2010, from http://www.markle.org/downloadable_assets/nstf_full.pdf

Markle Foundation Task Force. (2003). *Creating a trusted network for homeland security*. New York: Markle Foundation. Retrieved April 15, 2010, from http://www.markle.org/downloadable_assets/nstf_report2_full_report.pdf

Markle Foundation Task Force. (2006). *Mobilizing information to prevent terrorism: accelerating development of a trusted information sharing environment*. New York: Markle Foundation. April 16, 2010, from http://www.markle.org/downloadable_assets/2006_nstf_report3.pdf

Markle Foundation Task Force. (2009). *Nation at risk: Policymakers need better information to protect the country*. New York: Markle Foundation. Retrieved April 15, 2010, from http://www.markle.org/downloadable_assets/20090304_mtf_report.pdf

Miller, J. (2006, August 23). *Press release–Letter to Newsweek dated August 23, 2006.* Retrieved January 25, 2010, from http://www.fbi.gov/pressrel/pressrel06/millernewsweek.htm

Mines, M. C. (2007, September 27). *Federal Bureau of Investigation–Congressional Testimony- Statement of Michael C. Mines, Deputy Assistant Director, Directorate of Intelligence, Federal Bureau of Investigation, before the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, House Homeland Security Committee.* Retrieved September 1, 2010, from http://www.fbi.gov/congress/congress07/mines092707.htm

Mueller III, R. (2003, June 20). *"The FBI: Meeting new challenges" speech at the National Press Club on June 20, 2003.* Retrieved February 12, 2010, from http://www.fbi.gov/pressrel/speeches/npc062003.htm

Mueller III, R. (2005, February 3). Federal Bureau of Investigation Director, Statement before the United States Senate Committee on Appropriations Subcommittee on Commerce, Justice, State and the Judiciary on February 03, 2005: United States Senate Committee on Appropriations Subcommittee on Commerce, Justice, State and the Judiciary, United States Senate, (2005). Retrieved January 25, 2010, from http://www.fbi.gov/congress/congress05/mueller020305.htm

Mueller III, R. (2005, May 24). Federal Bureau of Investigation Director, statement before the Senate Committee on Appropriations Subcommittee on Commerce, Justice and Science on May 24, 2005: Committee on Appropriations, Subcommittee on Commerce, Justice and Science, U.S. Senate. Retrieved April 15, 2010, from http://www.fbi.gov/congress/congress05/mueller052405.htm

Mueller III, R. (2008, September 17). Federal Bureau of Investigation Director, Statement before the Senate Judiciary Committee on September 17, 2008: Judiciary Committee, U.S. Senate. Retrieved April 15, 2010, from http://www.fbi.gov/congress/congress08/mueller091708.htm

Mueller III, R. (2009, May 20). Federal Bureau of Investigation Director, Statement before the House Judiciary Committee on May 20, 2009: House Judiciary Committee, U.S. House of Representatives. Retrieved April 15, 2010, from http://www.fbi.gov/congress/congress09/mueller052009.htm

National Commission on Terrorist Attacks Upon the United States (9/11 Commission). (2004). *The 911 Commission report: Final report of the National Commission on Terrorist Attacks upon the United States* (1st ed.). New York: Norton.

National Counterterrorism Center (NCTC). (n.d.). *National Counterterrorism Center: About us.* Retrieved September 1, 2009, from http://www.nctc.gov/about_us/about_nctc.html

National Information Exchange Model (NIEM). (n.d.). *National Information Exchange Model (NIEM).* Retrieved October 11, 2009, from http://www.niem.gov/

National Institute of Standards and Technology (NIST). (n.d.). *NIST.gov–Computer security division–Computer security resource center.* Retrieved February 11, 2010, from http://csrc.nist.gov/groups/SMA/fisma/overview.html

Nelson, L. (2004). Privacy and Technology: Reconsidering a Crucial Public Policy Debate in the Post-September 11 Era. *Public Administration Review*, *64*(3), 259–269.

Nojeim, G. (2009, March 18). Director, Project on Freedom, Security & Technology, Center for Democracy & Technology on March 18, 2009: House Homeland Security Committee Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment, U.S. House of Representatives. Retrieved April 15, 2010, from http://homeland.house.gov/SiteDocuments/20090318101246-50012.pdf

Obama, B. H. (2009, May 27). *The White House–Press Office–Presidential Memorandum-Classified information and controlled unclassified information.* Retrieved September 20, 2009, from http://www.whitehouse.gov/the_press_office/Presidential-Memorandum-Classified-Information-and-Controlled-Unclassified-Information/

O'Hanlon, M. E. (2002). Protecting the American homeland: A preliminary analysis. *The Brookings Review*, *20*(3), 13–16.

Pelfrey, W. V. (2005). The cycle of preparedness: Establishing a framework to prepare for terrorist threats. *Journal of Homeland Security & Emergency Management*, *2*(1), 1–21.

Program Manager, Information Sharing Environment (PM-ISE). (2008). *Information Sharing Environment (ISE) Suspicious Activity Reporting (SAR) Evaluation Environment (EE) segment architecture*. Washington, DC: Program Manager, Information Sharing Environment (PM-ISE). Retrieved April 15, 2010, from http://www.ise.gov/docs/sar/ISE-SAR_EE_Segment_Architecture_v1(Dec_2008_Final).pdf

Program Manager, Information Sharing Environment (PM-ISE). (2009). *Information Sharing Environment progress and plans report to Congress 2009.* Retrieved April 15, 2010, from http://www.ise.gov/docs/reports/ISE_2009-Annual-Report_FINAL_2009-06-30.pdf

Regional Information Sharing System (RISS). (n.d.). *RISS overview.* Retrieved January 26, 2010, from http://www.riss.net/overview.aspx

Schäuble, W. (n.d.). *BMI Federal Minister of the Interior Wolfgang Schäuble explained that the Counter-terrorism Database is essential to the fight against terror.* Retrieved January 28, 2010, from http://www.en.bmi.bund.de/cln_012/nn_1016300/Internet/Content/Themen/Terrorism/DataAndFacts/Antiterrordatei__en.html

Sternstein, A. (2004). Secure flight starts taking names. *Federal Computer Week, 18*(34), 12.

Treverton, G. F. (2008). *Reorganizing U.S. domestic intelligence: Assessing the options*. 125. Retrieved April 15, 2010, from http://www.rand.org/pubs/monographs/2008/RAND_MG767.pdf

U.S. Department of Justice (DOJ). (2008). *Privacy impact assessment for the OneDOJ system (formerly the Regional Data Exchange System (R-DEx)*. Washington, DC: Department of Justice. Retrieved April 15, 2010, from http://www.justice.gov/jmd/pia/onedoj-pia.pdf

U.S. Department of Justice (DOJ). (n.d. (a)). *USDOJ: FY 2010 exhibit 300s.* Retrieved February 14, 2009, from http://www.justice.gov/jmd/2010justification/exhibit300/

U.S. Department of Justice (DOJ). (n.d. (b)). *USDOJ: LEISP: OneDOJ.* Retrieved February 1, 2010, from http://www.justice.gov/jmd/ocio/leisp/onedoj.htm

U.S. Department of Justice (DOJ). (n.d. (c)). *USDOJ:OPCL: Privacy impact assessments.* Retrieved February 5, 2010, from http://www.justice.gov/opcl/pia.htm

United States Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (WMD Commission). (2005). *The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction report.* Washington, DC: Author.

Wormeli, P., & Walter, A. A. (2009). Pass it on. *Fire Chief, 53*(8), 34.

Zhou, G., & Su, J. (2005). Machine learning-based named entity recognition via effective integration of various evidences. *Natural Language Engineering*, *11*(2), 189.

Zolin, R., Hinds, P. J., Fruchter, R., & Levitt, R. E. (2004). Interpersonal trust in cross-functional, geographically distributed work: A longitudinal study. *Information & Organization, 14*(1), 1.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, VA

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, CA

3. FBI Chief Information Sharing Officer
   FBIHQ
   Washington, DC